HITACHI
Inspire the Next

BladeSymphony BS500

マネジメントモジュールセットアップガイド

BS500007-25

登録商標・商標

HITACHI、BladeSymphony、Cosminexus、HiRDB、JP1、Virtage は、（株）日立製作所の商標または登録商標です。
Intel，インテル，Xeon は，アメリカ合衆国およびその他の国における Intel Corporation の商標です。
Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
Microsoft，Windows，Windows Server，Hyper-V は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Oracle と Java は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です。
Red Hat は，米国およびその他の国で Red Hat, Inc. の登録商標もしくは商標です。
VMware は、米国およびその他の地域における VMware, Inc.の登録商標または商標です。
その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

発行

2015 年 9 月（第 25 版）

版権

このマニュアルの内容はすべて著作権によって保護されています。このマニュアルの内容の一部または全部を，無断で転載することは禁じられています。
Copyright ⓒ Hitachi,Ltd.2012,2015,All rights reserved.

目次

はじめに 13
お知らせ 14
重要なお知らせ 14
システム装置の信頼性について 14
規制・対策などについて 14
このマニュアルで使用している記号 15
安全にお使いいただくために 16
安全に関する注意事項 16
安全に関する共通的な注意について 17
操作や動作は 17
自分自身でもご注意を 17
一般的な安全上の注意事項 17
オペレーティングシステム（OS）の略称について 23

1. マネジメントモジュールの概要 25
1.1 概要 26
1.2 マネジメントモジュールへの接続 26
1.2.1 マネジメントモジュールの外部インタフェース 26
1.2.2 マネジメントモジュールへのケーブル接続 28
1.3 機能一覧 29

2. 機能詳細 33
2.1 ユーザ管理 35
2.1.1 アカウントの概要 35
2.1.2 アカウントの設定 35
2.1.3 パスワード有効期限の設定 36
2.1.4 ロールの概要 37
2.1.5 ロールの設定 38
2.1.6 LCD タッチコンソールの認証について 38
2.2 時刻 39
2.2.1 マネジメントモジュールの時刻設定 39
2.2.2 NTP サーバ連携 40
2.2.3 システム装置の時刻管理方式 40
2.3 ネットワーク 41
2.3.1 各モジュールの管理用インタフェースで使用可能な機能一覧 42
2.3.2 管理ネットワーク 42
2.3.3 内部ネットワーク 43
2.3.4 スイッチモジュールの管理用インタフェース接続 43

2.3.5 接続方式の設定 45
2.3.6 IP アドレスの設定 48
2.3.7 マネジメントモジュール障害時のネットワーク構成 53
2.3.8 Link Fault Tolerance(LFT) 54
2.4 セキュリティ 55
2.4.1 マネジメントモジュールと BMC が提供する機能 56
2.4.2 セキュリティ強度設定 58
2.4.3 セキュリティ強度と各機能との関係 59
2.4.4 セキュリティ強度の設定による機能比較 60
2.4.5 TLS/SSL バージョン設定機能 63
2.4.6 マネジメントモジュールが提供するサービスの IP アドレス制限設定 65
2.4.7 認証情報暗号化設定 66
2.5 システム装置設定 66
2.5.1 シャーシ ID 設定 67
2.5.2 言語設定 67
2.6 電源制御 67
2.6.1 システム装置の電源を入れる 68
2.6.2 システム装置の電源を切る 68
2.6.3 サーバブレードの電源を操作する 68
2.6.4 スイッチモジュールの電源を操作する 69
2.6.5 電源復旧時のサーバブレード動作設定 69
2.7 サーバブレードの遠隔操作 70
2.7.1 リモートコンソールによる操作 70
2.7.2 OS コンソールによる操作 70
2.7.3 OS コンソール使用前の準備 70
2.7.4 OS コンソールの使用方法 72
2.7.5 OS コンソールの使用時の注意事項 72
2.8 識別 LED(LID)の操作 73
2.9 装置内の各モジュールの設定 74
2.9.1 マネジメントモジュールから実施可能な各モジュールの設定 74
2.9.2 サーバブレード(BMC 設定) 76
2.9.3 サーバブレード(UEFI 設定) 77
2.9.4 Hitachi LAN スイッチモジュールの設定 77
2.9.5 Hitachi ファイバチャネル拡張カードの設定 77
2.10 本装置における WWN，MAC アドレスについて 77
2.10.1 WWN，MAC アドレスの種別 77
2.10.2 WWN，MAC アドレスの種別に関する注意事項 78
2.10.3 Basic モードでの WWN，MAC アドレスの選択 81
2.10.4 HVM モードでの WWN，MAC アドレスの選択 81
2.10.5 N+M コールドスタンバイと WWN，MAC アドレスの関係 81
2.10.6 additional WWN，additional MAC アドレスの初期化 82
2.10.7 WWN，MAC アドレスの確認方法 82
2.10.8 additional WWN，additional MAC アドレスの変更ログ 84
2.11 ホスト情報の表示 85
2.12 JP1/ServerConductor/Blade Server Manager 連携 86
2.12.1 通知先 BSM の設定 86
2.13 HCSM 連携 87
2.13.1 HCSM からのディスカバリについて 88
2.13.2 HCSM 連携のオプション設定 89
2.14 N+M コールドスタンバイ 90
2.14.1 N+M コールドスタンバイ概要 90
2.14.2 N+M コールドスタンバイの仕組み 92
2.14.3 N+M コールドスタンバイで引き継ぐサーバブレードの設定情報 93
2.14.4 N+M 切り替え時間について 96

2.14.5 N+M コールドスタンバイの前提条件 96
2.14.6 N+M コールドスタンバイ使用時の注意事項 98
2.14.7 N+M コールドスタンバイにおける Pre-configure 99
2.14.8 Pre-configure 実行契機 100
2.14.9 Pre-configure 実行中のサーバブレードの動作 101
2.14.10 Pre-configure 実行所要時間 101
2.14.11 N+M コールドスタンバイ構築手順 101
2.14.12 N+M コールドスタンバイ構築後の設定変更 105
2.14.13 N+M コールドスタンバイ構築後の CNA 交換 105
2.14.14 N+M コールドスタンバイの UPS 接続設定 105
2.15 HA モニタ連携 106
2.15.1 HA モニタ概要 106
2.15.2 系切り替え構成の設定方法 107
2.16 LDAP 連携 112
2.16.1 概要 112
2.16.2 サポートする LDAP サーバ 113
2.16.3 Active Directory の設定(Windows 側の設定) 113
2.16.4 マネジメントモジュールへの設定 122
2.17 RADIUS 認証 123
2.17.1 概要 123
2.17.2 サポートする RADIUS サーバ 124
2.17.3 RADIUS サーバへの設定 124
2.17.4 マネジメントモジュールへの設定 124
2.17.5 RADIUS サーバ接続確認 125
2.18 Web コンソールにおけるデジタル証明書の利用 125
2.18.1 概要 125
2.18.2 デジタル証明書利用の諸元 126
2.18.3 デジタル証明書利用の手順(自己署名証明書を使用する場合) 126
2.18.4 デジタル証明書利用の手順(認証局に署名されたデジタル証明書を使用する場合) 127
2.19 HVM 連携 128
2.19.1 HVM 初期設定 130
2.19.2 HVM ファームウェアの選択 139
2.19.3 仮想 WWN の確認 142
2.19.4 仮想 MAC アドレスの確認 143
2.19.5 電源の投入 145
2.19.6 LPAR 作成 148
2.19.7 HVM 構成情報の保存 154
2.19.8 LPAR への USB 割り当ての設定 156
2.19.9 LPAR のブートオーダ設定 157
2.19.10 LPAR の Activate 170
2.19.11 リモートコンソールの呼び出し 172
2.19.12 LPAR の Reactivate 174
2.19.13 LPAR の Deactivate 177
2.19.14 LPAR 設定の変更 179
2.19.15 LPAR の削除 182
2.19.16 HVM の再起動 185
2.19.17 HVM のシャットダウン 187
2.19.18 HVM 設定のバックアップ 190
2.19.19 HVM 設定のリストア 192
2.19.20 HVM 設定の初期化 195
2.19.21 HVM のモデルアップ 197
2.19.22 HVM ファームウェアのアップデート 203
2.19.23 HVM ファームウェアのアンインストール 219
2.19.24 HVM 稼働時ダンプの採取 221
2.20 省電力機能 224
2.20.1 電力制限機能の管理 224

2.20.2 設備保護電力制御機能 225
2.20.3 運用時電力制御機能 227
2.20.4 サーバブレードに対する電力制御の無効設定 230
2.20.5 電源容量拡張機能 232
2.20.6 電力値のモニタリング表示 235
2.20.7 電源容量超過時のサーバブレード強制電源 OFF 順序設定 235
2.20.8 電源モジュール最適制御機能 235
2.21 DCMI 機能 236
2.21.1 DCMI 概要 236
2.21.2 DCMI に対応するサーバブレード 236
2.21.3 DCMI モードの設定方法 236
2.21.4 対応 DCMI コマンド一覧 237
2.22 静音モード機能 239
2.22.1 静音モード機能概要 239
2.23 SNMP 機能 240
2.23.1 SNMP 機能概要 240
2.23.2 前提条件 242
2.23.3 SNMP 機能の設定手順 242
2.23.4 SNMP トラップメッセージの選択 245
2.24 E-mail 通報機能 245
2.24.1 E-mail 機能概要 245
2.24.2 前提条件 246
2.24.3 E-mail 通報機能諸元 246
2.24.4 E-mail 通報機能の設定手順 247
2.24.5 手動契機通報(現状通報) 248
2.25 バナー機能 250
2.25.1 ログインバナー機能 250
2.26 USB ポートの無効化機能 252
2.27 インポート機能 252
2.27.1 インポート機能の概要 252
2.27.2 インポート実施方法 253
2.27.3 インポートファイルの書式と変更方法 259
2.27.4 インポート失敗時のトラブルシューティング 263
2.28 ログ 265
2.28.1 マネジメントモジュールから参照可能なログ 265
2.28.2 ダンプログ 266
2.28.3 操作ログ／監査ログ 267
2.28.4 操作ログ／監査ログメッセージ一覧 271
2.29 ファームウェア 279
2.29.1 マネジメントモジュールからアップデート可能なファームウェア 279
2.29.2 マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート 279
2.29.3 サーバブレードファームウェアのアップデート 289
2.30 設定の保存と復元 297
2.30.1 マネジメントモジュールから保存，復元可能な設定 297
2.30.2 マネジメントモジュール設定 297
2.30.3 Hitachi ファイバチャネル拡張カード設定 298
2.30.4 HVM 設定 298

3. ソフトウェアのライセンス情報 301
3.1 ソフトウェアのライセンス情報 302

付録 A HCSM アラートメッセージ一覧 309
A.1 HCSM アラートメッセージ一覧 310

図目次

図 1-1 マネジメントモジュールのポート位置 27
図 1-2 システムコンソールとマネジメントモジュールの接続（LAN ケーブル） 28
図 1-3 システムコンソールとマネジメントモジュールの接続（シリアルケーブル） 29
図 2-1 NTP サーバの連携イメージ 40
図 2-2 マネジメントモジュールの時刻同期イメージ 41
図 2-3 リセットパスの構成例 1 109
図 2-4 リセットパスの構成例 2 109
図 2-5 リセットパスの構成例 3 110
図 2-6 リセットパスの構成例 4 111
図 2-7 リセットパスのポート番号の具体的な設定例 111
図 2-8 LCD タッチコンソールを使用したときの例 253
図 2-9 成功時の表示画面 255
図 2-10 失敗時の表示画面 255
図 2-11 アップデートの流れ 290

表目次

表 1-1 マネジメントモジュールのポート種 27
表 1-2 マネジメントモジュールのネットワーク設定（工場出荷時） 27
表 1-3 ターミナルソフトウェアの通信パラメータ設定 28
表 1-4 主な機能一覧 29
表 2-1 工場出荷時のデフォルト値 35
表 2-2 Web コンソールでの操作方法 36
表 2-3 CLI コンソールでの操作方法 36
表 2-4 パスワード有効期限管理の工場出荷時の設定 37
表 2-5 Web コンソールでの操作方法 37
表 2-6 CLI コンソールでの操作方法 37
表 2-7 権限の一覧 37
表 2-8 組み込みロール 38
表 2-9 Web コンソールでの操作方法 38
表 2-10 CLI コンソールでの操作方法 38
表 2-11 Web コンソールでの操作方法 39
表 2-12 LCD タッチコンソールでの操作方法 39
表 2-13 CLI コンソールでの操作方法 39
表 2-14 Web コンソールでの操作方法 39
表 2-15 CLI コンソールでの操作方法 39
表 2-16 LCD タッチコンソールでの操作方法 40
表 2-17 Web コンソールでの操作方法 40
表 2-18 Web コンソールでの操作方法 41
表 2-19 Web コンソールでの操作方法 43
表 2-20 Web コンソールでの操作方法 45
表 2-21 接続方式の工場出荷時の設定 46
表 2-22 Web コンソールでの操作方法 46
表 2-23 CLI コンソールでの操作方法 46
表 2-24 IP アドレスの工場出荷時の設定 48
表 2-25 Web コンソールでの操作方法 49
表 2-26 CLI コンソールでの操作方法 50
表 2-27 LCD タッチコンソールでの操作方法 50
表 2-28 Web コンソールでの操作方法 53
表 2-29 CLI コンソールでの操作方法 53
表 2-30 Web コンソールでの操作方法 55
表 2-31 マネジメントモジュールが提供する機能 56
表 2-32 BMC が提供する機能 57
表 2-33 Web コンソールでの操作方法 58

表 2-34 CLI コンソールでの操作方法 58
表 2-35 Web コンソールでの操作方法 64
表 2-36 CLI コンソールでの操作方法 64
表 2-37 Web コンソールでの操作方法 65
表 2-38 CLI コンソールでの操作方法 65
表 2-39 LCD タッチコンソールでの操作方法 66
表 2-40 CLI コンソールでの操作方法 66
表 2-41 Web コンソールでの操作方法 67
表 2-42 CLI コンソールでの操作方法 67
表 2-43 Web コンソールでの操作方法 67
表 2-44 CLI コンソールでの操作方法 67
表 2-45 Web コンソールでの操作方法 68
表 2-46 CLI コンソールでの操作方法 68
表 2-47 LCD タッチコンソールでの操作方法 68
表 2-48 Web コンソールでの操作方法 69
表 2-49 CLI コンソールでの操作方法 69
表 2-50 Web コンソールでの操作方法 69
表 2-51 Web コンソールでの操作方法 70
表 2-52 CLI コンソールでの操作方法 70
表 2-53 COM2 のポート設定 71
表 2-54 パラメータ設定例 71
表 2-55 CLI コンソールでの操作方法 72
表 2-56 現象と対処方法 73
表 2-57 シーケンスの送信内容 73
表 2-58 Web コンソールでの操作方法 73
表 2-59 CLI コンソールでの操作方法 74
表 2-60 LCD タッチコンソールでの操作方法 74
表 2-61 Web コンソールから実施可能な各モジュールの設定項目 75
表 2-62 CLI コンソールから実施可能な各モジュールの設定項目 75
表 2-63 Web コンソールでの操作方法 76
表 2-64 CLI コンソールでの操作方法 76
表 2-65 Personality 設定/MultiChannel Support 設定の制限事項 79
表 2-66 Web コンソールでの操作方法 81
表 2-67 CLI コンソールでの操作方法 81
表 2-68 Web コンソールでの操作方法 82
表 2-69 Web コンソールでの操作方法 83
表 2-70 CLI コンソールでの操作方法 83
表 2-71 Emulex 10Gb CNA 拡張カードまたはオンボード CNA(2 ポート)の場合 84
表 2-72 Emulex 10Gb オンボード CNA(4 ポート)の場合 84
表 2-73 Web コンソールでの操作方法 85
表 2-74 CLI コンソールでの操作方法 85
表 2-75 表示可能ホスト情報 85
表 2-76 Web コンソールでの操作方法 86
表 2-77 Web コンソールでの操作方法 87
表 2-78 Web コンソールでの操作方法 89
表 2-79 CLI コンソールでの操作方法 89
表 2-80 Web コンソールでの操作方法 90
表 2-81 CLI コンソールでの操作方法 90
表 2-82 引き継ぎ区分と項目 94
表 2-83 引き継ぎ区分と項目 95
表 2-84 ファームウェアバージョンとドライバの構成 98

表 2-85 Web コンソールでの操作方法 100
表 2-86 Web コンソールでの操作方法 101
表 2-87 Web コンソールでの操作方法 102
表 2-88 Web コンソールでの操作方法 102
表 2-89 Web コンソールでの操作方法 105
表 2-90 Web コンソールでの操作方法 106
表 2-91 Web コンソールでの操作方法 106
表 2-92 Web コンソールでの操作方法 107
表 2-93 系切り替え構成のリセットパスのポート番号 111
表 2-94 Active Directory の設定項目 113
表 2-95 ユーザ名として使用できる文字および文字長 118
表 2-96 パスワードとして使用できる文字および文字長 118
表 2-97 Web コンソールでの操作方法 123
表 2-98 CLI コンソールでの操作方法 123
表 2-99 Web コンソールにおけるデジタル証明書利用の諸元 126
表 2-100 Web コンソールでの操作方法 128
表 2-101 Web コンソールと Virtage Navigator の機能一覧 128
表 2-102 電力制限機能に関連する設定項目 224
表 2-103 Web コンソールでの操作方法 227
表 2-104 CLI コンソールでの操作方法 227
表 2-105 Web コンソールでの操作方法 228
表 2-106 CLI コンソールでの操作方法 228
表 2-107 Web コンソールでの操作方法 230
表 2-108 CLI コンソールでの操作方法 230
表 2-109 Web コンソールでの操作方法 235
表 2-110 Web コンソールでの操作方法 235
表 2-111 CLI コンソールでの操作方法 235
表 2-112 Web コンソールでの操作方法 235
表 2-113 Web コンソールでの操作方法 236
表 2-114 CLI コンソールでの操作方法 236
表 2-115 Web コンソールでの操作方法 237
表 2-116 CLI コンソールでの操作方法 237
表 2-117 対応 DCMI コマンド一覧 237
表 2-118 Web コンソールでの操作方法 239
表 2-119 SNMP 機能 240
表 2-120 SNMP ポーリング機能の諸元 241
表 2-121 SNMP トラップ機能の諸元 241
表 2-122 SNMPv3 機能の諸元 242
表 2-123 Web コンソールでの操作方法 242
表 2-124 CLI コンソールでの操作方法 243
表 2-125 Web コンソールでの操作方法 244
表 2-126 CLI コンソールでの操作方法 244
表 2-127 Web コンソールでの操作方法 244
表 2-128 CLI コンソールでの操作方法 244
表 2-129 Web コンソールでの操作方法 245
表 2-130 CLI コンソールでの操作方法 245
表 2-131 E-mail 通報機能の諸元 246
表 2-132 添付ファイルの諸元 247
表 2-133 Web コンソールでの操作方法 248
表 2-134 CLI コンソールでの操作方法 248
表 2-135 Web コンソールでの操作方法 249

表 2-136 CLI コンソールでの操作方法 249
表 2-137 手動契機通報結果メッセージ一覧 249
表 2-138 Web コンソールでの操作方法 251
表 2-139 Web コンソールでの操作方法 252
表 2-140 CLI コンソールでの操作方法 252
表 2-141 マネジメントモジュールから参照可能なログ 265
表 2-142 Web コンソールでの操作方法 265
表 2-143 CLI コンソールでの操作方法 266
表 2-144 LCD タッチコンソールでの操作方法 266
表 2-145 操作ログ／監査ログの諸元 267
表 2-146 操作ログのフォーマット 268
表 2-147 操作イベント種別表 269
表 2-148 操作イベント結果表 269
表 2-149 監査ログのフォーマット 269
表 2-150 マネジメントモジュールの操作ログ／監査ログメッセージ一覧 271
表 2-151 サーバブレードの操作ログ／監査ログメッセージ一覧 278
表 2-152 ファームウェアの種類 279
表 2-153 アップデート対象一覧 279
表 2-154 バージョンアップ作業中の禁止事項 280
表 2-155 電源 ON 実行中や電源 OFF 実行中の禁止事項 281
表 2-156 アラート 281
表 2-157 アラート 281
表 2-158 メッセージの通知 281
表 2-159 Web コンソールでの操作方法 282
表 2-160 CLI コンソールでの操作方法 282
表 2-161 LCD タッチコンソールでの操作方法 283
表 2-162 複数台同時アップデートの実施可否 289
表 2-163 Web コンソールでの操作方法 291
表 2-164 CLI コンソールでの操作方法 291
表 2-165 LCD タッチコンソールでの操作方法 291
表 2-166 保存と復元 297
表 2-167 Web コンソールでの操作方法 297
表 2-168 Web コンソールでの操作方法 298
表 2-169 CLI コンソールでの操作方法 298
表 2-170 Web コンソールでの操作方法 298
表 2-171 Web コンソールでの操作方法 299
表 3-1 オープンソースソフトウェア 302

はじめに

マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の指示をよく読み，十分理解してください。

このマニュアルは，いつでも参照できるよう，手近なところに保管してください。

- お知らせ
- このマニュアルで使用している記号
- 安全にお使いいただくために
- オペレーティングシステム（OS）の略称について

お知らせ

重要なお知らせ

- 本書の内容の一部，または全部を無断で転載したり，複写することは固くお断わりします。
- 本書の内容について，改良のため予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが，万一ご不審な点や誤りなど，お気付きのことがありましたら，お買い求め先へご一報くださいますようお願いいたします。
- 本書に準じないで本製品を運用した結果については責任を負いかねますので，あらかじめご了承ください。
- この製品には，RSA Data Security からライセンスを受けたコードが含まれています。

システム装置の信頼性について

ご購入いただきましたシステム装置は，一般事務用を意図して設計・製作されています。生命，財産に著しく影響のある高信頼性を要求される用途への使用は避けてください。このような使用に対する万一の事故に対し，弊社は一切責任を負いません。

高信頼性を必要とする場合には別システムが必要です。弊社営業部門にご相談ください。

一般事務用システム装置が不適当な，高信頼性を必要とする用途例

- 化学プラント制御・医療機器制御・緊急連絡制御等

規制・対策などについて

電波障害自主規制について

電波障害自主規制については，次の説明文をお読みください。

この装置は，クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
VCCI-A

電源の瞬時電圧低下対策について

本装置は，落雷などによる電源の瞬時電圧低下に対して不都合が生じることがあります。電源の瞬時電圧低下対策としては，交流無停電電源装置等を使用されることをお勧めします。

高調波電流規格：JIS C 61000-3-2 準用品について

JIS C61000-3-2 準用品とは，日本工業規格「電磁両立性－第 3-2 部：限度値－高調波電流発生限度値(1 相当たりの入力電流が 20A 以下の機器)」を準用し，商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

雑音耐力について

本製品の外来電磁波に対する耐力は，国際電気標準会議規格 IEC61000-4-3「放射無線周波電磁界イミュニティ試験」のレベル 2 に相当する規定に合致していることを確認しております。

輸出規制について

本製品を輸出される場合には，外国為替および外国貿易法並びに米国の輸出管理関連法規などの規制をご確認のうえ，必要な手続きをお取りください。なお，ご不明の場合は弊社担当営業にお問い合わせください。なお，この装置に付属する周辺機器やプレインストールされているソフトウェアも同じ扱いになります。

システム装置の廃棄・譲渡時のデータ消去に関するご注意

最近，パソコンやシステム装置はオフィスや家庭などで，いろいろな用途に使われるようになってきています。これらのシステム装置の中のハードディスクという記憶装置に，お客様の重要なデータが記録されています。

したがって，そのシステム装置を譲渡あるいは廃棄するときには，これらの重要なデータ内容を消去するということが必要となります。

ところが，このハードディスクに書き込まれたデータを消去するというのは，それほど簡単ではありません。「データを消去する」という場合，一般に

- データを「ゴミ箱」に捨てる
- 「削除」処理を行う
- 「ゴミ箱を空にする」コマンドを使って消す
- ソフトで初期化（フォーマット）する

などの作業をすると思いますが，これらのことをしても，ハードディスク内に記録されたデータのファイル管理情報が変更されるだけで，実際はデータは見えなくなっているという状態なのです。

つまり，一見消去されたように見えますが，Windows® などの OS のもとで，それらのデータを呼び出す処理ができなくなっただけで，本来のデータは残っているという状態にあるのです。

したがって，特殊なデータ回復のためのソフトウェアを利用すれば，これらのデータを読みとることが可能な場合があります。このため，悪意のある人により，このシステム装置のハードディスク内の重要なデータが読みとられ，予期しない用途に利用されるおそれがあります。システム装置ユーザが，廃棄・譲渡などを行う際に，ハードディスク上の重要なデータが流出するというトラブルを回避するためには，ハードディスクに記録された全データを，ユーザの責任において消去することが非常に重要となります。消去するためには，専用ソフトウェアあるいはサービス（共に有償）を利用するか，ハードディスク上のデータを金槌や強磁気により物理的・磁気的に破壊して，読めなくすることを推奨します。

なお，ハードディスク上のソフトウェア（OS，アプリケーションソフトなど）を削除することなくシステム装置を譲渡すると，ソフトウェアライセンス使用許諾契約に抵触する場合があるため，十分な確認を行う必要があります。

ハードディスクのデータを消去するユーティリティは，『CLEAR-DA』，『CLEAR-DA RAID』などがあります。詳細は担当営業へお問い合わせください。

制限

『CLEAR-DA』は，CD より起動させて使用します。

本システム装置については，別途 USB 外付け CD 装置が必要となります。

このマニュアルで使用している記号

このマニュアルでは，次に示すアイコンを使用します。

アイコン	ラベル	説明
警告	警告	これは，死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
注意	注意	これは，軽度の傷害，あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
通知	通知	これは，装置の重大な損傷，または周囲の財物の損傷を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
重要	重要	重要情報や追加情報，および装置やソフトウェアの制限事項を説明します。
参考	参考	より効率的に業務を行うために，知っておくと役に立つ情報や指針となる情報を説明します。

このマニュアルでは，次に示す記号を使用しています。

記号	意味
[ ] （角括弧）	GUI 操作の説明 メニュータイトル，メニュー項目，タブ名，およびボタンの名称を示します。メニュー項目を連続して選択する場合は，[ ] を「ー」（ハイフン）でつないで説明しています。 キー操作の説明 キーの名称を示します。
斜体文字	次のどちらかを示します。 • 可変値であることを示します。 • ドキュメントタイトルであることを示します。

安全にお使いいただくために

安全に関する注意事項

この項で説明する安全に関する注意事項は，下に示す見出しによって表示されます。これは安全警告記号と「警告」，「注意」および「通知」という見出し語を組み合わせたものです。

これは，安全警告記号です。人への危害をひき起こす隠れた危険に注意を喚起するために用いられます。起こりうる傷害または死を回避するためにこのシンボルの後に続く安全に関するメッセージに従ってください。

警告

これは，死亡または重大な傷害をひき起こすおそれのある危険の存在を示すのに用いられます。

注意

これは，軽度の傷害，あるいは中程度の傷害をひき起こすおそれのある危険の存在を示すのに用いられます。

通知

これは，人身傷害とは関係のない損害をひき起こすおそれのある危険の存在を示すのに用いられます。

【表記例 1】感電注意

の図記号は注意していただきたいことを示し，の中に「感電注意」などの注意事項の絵が描かれています。

【表記例 2】分解禁止

の図記号は禁止事項を示し，の中に「分解禁止」などの禁止事項の絵が描かれています。なお，の中に絵がないものは，一般的な禁止事項を示します。

【表記例 3】電源プラグをコンセントから抜け

の図記号は行っていただきたいことを示し，の中に「電源プラグをコンセントから抜け」などの強制事項の絵が描かれています。なお，は一般的に行っていただきたい事項を示します。

安全に関する共通的な注意について

次に述べられている安全上の説明をよく読み，十分理解してください。

- 操作は，このマニュアル内の指示，手順にしたがって行ってください。
- 本製品やマニュアルに表示されている注意事項は必ず守ってください。
- 本製品に搭載または接続するオプションなど，ほかの製品に添付されているマニュアルも参照し，記載されている注意事項を必ず守ってください。

これを怠ると，けが，火災や装置の破損を引き起こすおそれがあります。

操作や動作は

マニュアルに記載されている以外の操作や動作は行わないでください。

本製品について何か問題がある場合は，電源を切り，電源プラグをコンセントから抜いたあと，お買い求め先にご連絡いただくか保守員をお呼びください。

自分自身でもご注意を

本製品やマニュアルに表示されている注意事項は，十分検討されたものです。それでも，予測を超えた事態が起こることが考えられます。操作に当たっては，指示にしたがうだけでなく，常に自分自身でも注意するようにしてください。

一般的な安全上の注意事項

本製品の取り扱いにあたり次の注意事項を常に守ってください。

電源ケーブルの扱い

電源ケーブルは必ず付属のものを使用し，次のことに注意して取り扱ってください。取り扱いを誤ると，電源コードの銅線が露出し，ショートや一部断線で過熱して，感電や火災の原因になります。

- 物を載せない
- 熱器具のそばで使用しない
- 加熱しない
- 束ねない
- 紫外線や強い可視光線を連続して当てない
- コードに傷がついた状態で使用しない
- 高温環境で使用しない
- 定格以上で使用しない
- ほかの装置で使用しない
- 電源プラグを濡れた手で触らない

なお，電源プラグはすぐに抜けるよう，コンセントの周りには物を置かないでください。

電源プラグの接触不良やトラッキング

電源プラグは次のようにしないと，トラッキングの発生や接触不良で過熱し，火災の原因となります。

- 電源プラグは根元までしっかり差し込んでください。
- 電源プラグはほこりや水滴が付着していないことを確認し，差し込んでください。
  付着している場合は乾いた布などで拭き取ってから差し込んでください。

電源コンセントの扱い

- 電源コンセントは接地型 2 極差し込みコンセントをご使用ください。その他のコンセントを使用すると感電や火災の原因になります。
- コンセントの接地極は，感電防止のために，アース線を専門の電気技術者が施工したアース端子に接続してください。接続しないと，万一電源の故障時などに感電するおそれがあります。

電源プラグの抜き差し

電源プラグをコンセントに差し込むとき，または抜くときは必ず電源プラグを持って行ってください。電源コードを引っ張るとコードの一部が断線してその部分が過熱し，火災の原因になります。

電源モジュールについて

電源モジュールは，高電圧部分が内部にあるためカバーを開けないでください。感電や装置の故障の原因になります。

電源スロットカバーの取り付け

電源ユニットの取り外し時，手や工具を内部に差し入れないでください。また，取り外し後は電源スロットカバーを取り付けてください。電源スロット内部には導体が露出した部分があり，万一手や工具などで触れると感電や装置の故障の原因になります。

異常な熱さ，煙，異常音，異臭

万一異常が発生した場合は，電源を切り，装置のすべて（最大 4 本）の電源プラグをコンセントから抜いてください。

修理・改造・分解

本書の指示にしたがって行うオプションなどの増設作業を除いては，自分で修理や改造・分解をしないでください。感電や火災，やけどの原因になります。特に電源ユニット内部は高電圧部が数多くあり，万一さわると危険です。

カバー・ブラケットの取り外し

カバー・ブラケットの取り外しは行わないでください。感電ややけど，または装置の故障の原因となります。

電源モジュールのカバーの高温について

電源モジュールは動作時カバーやハンドルが熱くなっています。障害が発生したモジュールを交換する場合などはご注意ください。やけどをするおそれがあります。

10GBASE-R トランシーバの高温について

1/10Gbps LAN スイッチモジュールの 10GBASE-R トランシーバは，動作時に熱くなっています。トランシーバの取り外しは，マネジメントモジュールから 10Gbps LAN スイッチモジュールの電源を停止してから約 5 分以上，時間をおいてから行ってください。やけどの原因になります。

装置内部品の追加・交換

電源を切った直後は，カバーや内部の部品が熱くなっています。本マニュアルで指示のない限り装置内部品の追加・交換は，電源を切った直後約 30 分，時間をおいてから行ってください。やけどの原因になります。

レーザー光について

- 本製品に搭載されているレーザーは，クラス 1 レーザー製品です。レーザー光を直視しないようにしてください。光学器械を用いてレーザー光を見ないようにしてください。

- レーザーモジュールのカバーを外すと，レーザー光が発射されています。使用していないボードのカバーは外さないようにしてください。

製品の取り扱い

- 製品は固定したラックに搭載してください。製品に寄りかかったり，上に乗ったりしないでください。また，床や壁などが弱い場所には設置しないでください。
- 過度な振動は与えないでください。落ちたり倒れたり，故障の原因となります。

ラック搭載について

- システム装置をラックキャビネットに取り付けたり取り外したりする場合は，必ず 2 人以上で作業を行い，無理をせず器具などを使用してください。また，ラックキャビネットの 31U 以上にシステム装置を取り付けたり，取り付けられている場合は，作業は行わず，保守員にお任せください。取り付け不備によりシステム装置が落下し，怪我をしたり装置が故障するおそれがあります。
- ラックキャビネットから装置を引き出して作業を行う場合，必ずラックキャビネットにスタビライザーを取り付けてください。無理な力がかかるとラックキャビネットが転倒し，怪我や故障の原因になります。取り付けられていない場合は保守員をお呼びください。

ラックキャビネット搭載時の取り扱い

ラックキャビネット搭載時，装置上面の空きエリアを棚または作業空間として使用しないでください。装置上面の空きエリアに重量物を置くと，落下による怪我の原因となります。

金属など端面への接触

装置の移動，部品の追加などで金属やプラスチックなどの端面に触れる場合は，注意して 触れてください。けがをするおそれがあります。

不適切なバッテリー

不正な種類のバッテリーと交換すると爆発の危険があります。

使用済みのバッテリーは指示にしたがって廃棄してください。

電池の取り扱い

電池の交換は保守員が行います。交換は行わないでください。また，次のことに注意してください。取り扱いを誤ると過熱・破裂・発火などでけがの原因となります。

- 充電しない
- ショートしない
- 分解しない

バッテリーの保管

バッテリーを保管する際は，バッテリー端子に接着テープを貼付して絶縁してください。絶縁しないと，端子同士の接触によりショートして，過熱や破裂を引き起こすことがあり，怪我や火災につながります。

装置内部への異物の混入

通気孔などから，内部にクリップや虫ピンなどの金属類や燃えやすい物などを入れないでください。そのまま使用すると，故障の原因になります。

落下などによる衝撃

落下させたりぶつけるなど，過大な衝撃を与えないでください。内部に変形や劣化が生じ，そのまま使用すると故障の原因になります。

通気孔

通気孔は内部の温度上昇を防ぐためのものです。物を置いたり立てかけたりして通気孔をふさがないでください。内部の温度が上昇し，故障の原因になります。また，通気孔は常にほこりが付着しないよう，定期的に点検し，清掃してください。

接続端子への接触

コネクタなどの接続端子に手や金属で触れたり，針金などの異物を挿入したりしないでください。また，金属片のある場所に置かないでください。短絡が起きて故障の原因になります。

温度差のある場所への移動

移動する場所間で温度差が大きい場合は，表面や内部に結露することがあります。結露した状態で使用すると装置の故障の原因となります。すぐに電源を入れたりせず，使用する場所で数時間そのまま放置し，室温と装置内温度がほぼ同じに安定してからご使用ください。

たとえば，5℃の環境から 25℃の環境に持ち込む場合，2 時間ほど放置してください。

周辺機器の増設や接続

マニュアルの説明にしたがい，マニュアルで使用できることが明記された周辺機器をご使用ください。それ以外のものを使用すると，接続仕様の違いにより周辺機器や装置の故障の原因になります。

電波障害について

ほかのエレクトロニクス機器に隣接して設置した場合，お互いに悪影響を及ぼすことがあります。特に近くにテレビやラジオなどがある場合，雑音が入ることがあります。

強い磁気の発生体

磁石やスピーカーなどの強い磁気を発生するものを近づけないでください。システム装置の故障の原因になります。

ハードディスクの取り扱いについて

ハードディスクは精密機械です。ご使用にあたっては，大切に取り扱ってください。取り扱い方法によっては，ハードディスク故障の原因になります。

障害ディスクについて

障害ディスクの交換では，操作手順の誤りや交換ディスクの故障などにより，データが破壊されるおそれがあります。交換の前にデータのバックアップを取ってください。

アルミ電解コンデンサ

アルミ電解コンデンサは有寿命部品です。耐用期間を過ぎた製品は使用しないでください。耐用期間を過ぎた製品を使用した場合，電解質の漏洩や消耗により，発煙や感電を引き起こすことがあります。こうした危険な状況を起こさないために，所定の耐用期間を過ぎた有寿命部品は交換してください。

分電盤

分電盤は出入り口付近に設置して，コンピュータシステムのデバイスを保護し，緊急時の電源遮断器として使用してください。

信号ケーブルについて

- ケーブルは足などをひっかけないように配線してください。足をひっかけるとけがや接続機器の故障の原因になります。また，大切なデータが失われるおそれがあります。
- ケーブルの上に重量物を載せないでください。また，熱器具のそばに配線しないでください。ケーブル被覆が破れ，接続機器などの故障の原因になります。

電源を切る前に

- 電源操作は決められた手順にしたがって行ってください。決められた手順に従わずに電源を入れたり切ったりすると，システム装置の故障の原因になります。
- 電源を切る前に，装置に接続するすべてのデバイスが停止していることを確認してください。装置の稼働中に電源を切ると，装置が故障したり，データが消えることがあります。
- シャットダウンを必要とする OS を使用している場合は，電源を切る前に必ずシャットダウンを終了してください。シャットダウン終了前に電源を切ると，データが消えることがあります。

ラック搭載時の注意

- **周囲温度の上昇について**

  閉鎖型或いはマルチユニット型組み立てラックへ装置を搭載する場合は，装置稼働時のラック内温度が室内周辺温度より高くなることがあります。装置の最大定格周囲温度を超えないようにご注意ください。

- **エアフローの低下について**

  装置をラックに搭載する際は，装置の安全稼働に必要なエアフロー量が低下しないようご注意ください。

- **リフターによる搭載について**

  装置をリフターでラック搭載する際は，高低差のない水平な場所で作業を行い，危険な状態とならないようご注意ください。

- **過負荷について**

  装置への給電を行う際には，過電流による回路の遮断や電源ケーブルの発熱にご注意ください。このため，定格に十分注意して使用することが必要です。

- **接地の接続**

  ラック搭載装置は, 常に確実なアース接続を行ってください。分岐回路 (例: テーブル タップ) への電源接続で接地接続されない装置では，特にご注意ください。

オペレーティングシステム（OS）の略称について

本マニュアルでは，次の OS 名称を省略して表記します。

また，Service Pack については記載していません。

- Microsoft® Windows Server® 2012 R2 Standard 日本語版 （以下 Windows Server 2012 R2 Standard）
- Microsoft® Windows Server® 2012 R2 Datacenter 日本語版（以下 Windows Server 2012 R2 Datacenter）
- Microsoft® Windows Server® 2012 Standard 日本語版 （以下 Windows Server 2012 Standard）
- Microsoft® Windows Server® 2012 Datacenter 日本語版 （以下 Windows Server 2012 Datacenter）
- Microsoft® Windows Server® 2008 R2 Standard 日本語版（以下 Windows Server 2008 R2 Standard）
- Microsoft® Windows Server® 2008 R2 Enterprise 日本語版（以下 Windows Server 2008 R2 Enterprise）
- Microsoft® Windows Server® 2008 R2 Datacenter 日本語版（以下 Windows Server 2008 R2 Datacenter）
- Microsoft® Windows Server® 2008 Standard 日本語版（以下 Windows Server 2008 Standard）
- Microsoft® Windows Server® 2008 Enterprise 日本語版（以下 Windows Server 2008 Enterprise）
- Microsoft® Windows Server® 2008 Datacenter 日本語版（以下 Windows Server 2008 Datacenter）

- Microsoft® Windows Server® 2008 Standard 32-bit 日本語版（以下 Windows Server 2008 Standard 32-bit）
- Microsoft® Windows Server® 2008 Enterprise 32-bit 日本語版（以下 Windows Server 2008 Enterprise 32-bit）
- Microsoft® Windows Server® 2008 Datacenter 32-bit 日本語版（以下 Windows Server 2008 Datacenter 32-bit）
- Red Hat® Enterprise Linux® 6.2（以下 RHEL 6.2 または Linux 6.2）

なお次のとおり，省略した「OS 表記」は，「対象 OS」中のすべてまたは一部を表すときに用います。

OS 表記	対象 OS
Windows Server 2012 R2	• Windows Server 2012 R2 Standard • Windows Server 2012 R2 Datacenter
Windows Server 2012	• Windows Server 2012 Standard • Windows Server 2012 Datacenter
Windows Server 2008 R2	• Windows Server 2008 R2 Standard • Windows Server 2008 R2 Enterprise • Windows Server 2008 R2 Datacenter
Windows Server 2008	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2008 Datacenter • Windows Server 2008 Standard 32-bit • Windows Server 2008 Enterprise 32-bit • Windows Server 2008 Datacenter 32-bit
Windows Server 2008 64bit 版	• Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2008 Datacenter
Windows Server 2008 32bit 版	• Windows Server 2008 Standard 32-bit • Windows Server 2008 Enterprise 32-bit • Windows Server 2008 Datacenter 32-bit

1

マネジメントモジュールの概要

この章では，マネジメントモジュールの概要について説明します。

- 1.1 概要
- 1.2 マネジメントモジュールへの接続
- 1.3 機能一覧

1.1 概要

マネジメントモジュールは，システム装置の制御，環境監視などシステム装置全体を管理するハードウェアです。

本マニュアルでは，マネジメントモジュールおよび関連装置を使用した，システム装置の各種設定方法について説明します。

マネジメントモジュールは，システム装置内のサーバブレード，スイッチモジュール，電源モジュールおよびファンモジュールなどの各種モジュールの制御や環境監視を行い，システム装置全体を管理するハードウェアです。システム装置の異常を検出した場合，E-mail，SNMP などの手段で，管理者に通知することができます。

システム装置を管理サーバ(JP1/ServerConductor/Blade Server Manager，以下 BSM と略す)を使用して管理する場合，BSM とマネジメントモジュールが協調して動作し，システム装置の稼働状態管理，アラート通知，N+M コールドスタンバイなどの機能を実現します。

マネジメントモジュールは，システム装置の状態表示と設定を行うコンソールを提供します。コンソールには，次の 3 種類があります。

- Web コンソール
  詳しい使用方法は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。
- CLI(Command Line Interface)コンソール
  詳しい使用方法は「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。
- LCD(Liquid Crystal Display，液晶ディスプレイ)タッチコンソール
  詳しい使用方法は「*BladeSymphony BS500 LCD タッチコンソール ユーザーズガイド*」を参照してください。

LCD タッチコンソールを使用すると，システムコンソールレスでのシステム装置の設定が可能となります。

マネジメントモジュールのコンソールから，サーバブレード，スイッチモジュールなどの一元的な設定も可能です。マネジメントモジュールのコンソールに接続すれば，ほかのコンソールに接続することなく，シームレスにシステム装置内の各モジュールの設定を行うことができます。

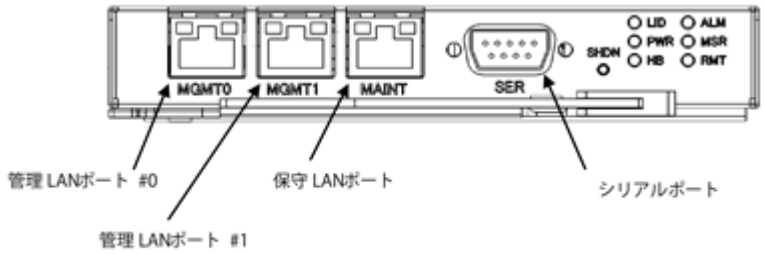
1.2 マネジメントモジュールへの接続

マネジメントモジュールの外部インタフェースと，ケーブル接続について説明します。

1.2.1 マネジメントモジュールの外部インタフェース

マネジメントモジュールは，外部ポートとして，管理 LAN ポート#0(MGMT0)，管理 LAN ポート#1(MGMT1)，保守 LAN ポート(MAINT)，シリアルポート(SER)を備えています。

図 1-1 マネジメントモジュールのポート位置



マネジメントモジュールのポート位置

表 1-1 マネジメントモジュールのポート種

ポート	説明
管理 LAN ポート#0(MGMT0)	管理ネットワークに接続するポートです。初期設定時は，このポートに接続します。
管理 LAN ポート#1(MGMT1)	管理ネットワークに接続するポートです。装置出荷時は，接続できません。詳しくは「2.3 ネットワーク」を参照してください。
保守 LAN ポート(MAINT)	保守用に保守員が利用する専用ポートです。ユーザは使用できません。
シリアルポート(SER)	システムコンソール用のシリアルポートです。LAN ポートが使用できない場合や，装置の初期設定などで使用します。

参考 LAN ポートで接続するためには，次に示すものを，お客様に用意していただく必要があります。

- システムコンソール
- UTP ケーブル（UTP-5 以上）
- HTTP，TELNET および SSH のいずれかのクライアントソフトウェア

マネジメントモジュールに HTTP，TELNET および SSH 接続する場合，マネジメントモジュールのネットワークの工場出荷時設定は次のとおりです。

表 1-2 マネジメントモジュールのネットワーク設定（工場出荷時）

項目	工場出荷時設定
IP アドレス	192.168.0.1
サブネットマスク	255.255.255.0
HTTPS	有効
HTTP	有効
SSH	有効
TELNET	有効

※　マネジメントモジュールのコンソールから設定変更可能です。

参考 シリアルポートで接続するためには，次に示すものをお客様に用意していただく必要があります。

- システムコンソール
- シリアルポート接続ケーブル（RS-232C クロスケーブル DSUB9 ピン メスーメスコネクタ）
- VT100 エミュレーション可能なターミナルソフト（ハイパーターミナルなど）

マネジメントモジュールのシリアルポートに接続する場合，ターミナルソフトウェアの通信パラメータ設定は次のとおりです。

表 1-3 ターミナルソフトウェアの通信パラメータ設定

通信パラメータ	設定内容
通信速度	9600bps
データ	8bit
パリティ	無し
ストップビット	1bit
フロー制御	無し

※　通信速度はマネジメントモジュールのコンソールから設定変更可能です。

シリアルポートの通信速度の設定は，主系のマネジメントモジュールから実行してください。

待機系のマネジメントモジュールにも同じ設定値が反映されます。

なお，変更したシリアルポートの通信速度を装置に反映するためには，シリアルポート接続からの logout 操作が必要です。（主系/待機系，各々必要です）

このため，シリアルポート経由で login した状態で通信速度を変更した場合は，一度 logout してください。

シリアルポート経由で login していない状態で(LAN ポート経由で)通信速度を変更した場合は，一旦変更前の通信速度で login していただき，その後 logout してください。

次の login より新しい通信速度となります。

参考 シリアルポートから Web コンソールは利用できません。

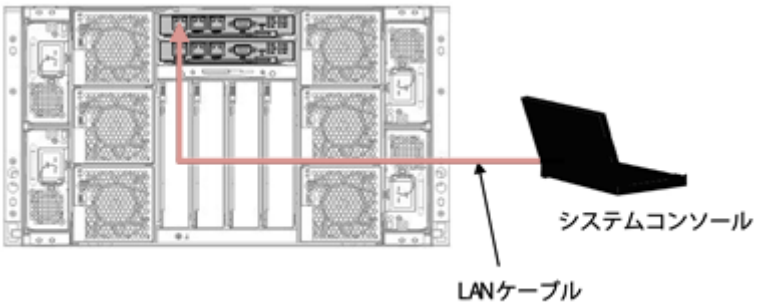
1.2.2 マネジメントモジュールへのケーブル接続

マネジメントモジュールへのケーブル接続について説明します。

(1)　LAN ケーブルでの接続

システム装置背面のマネジメントモジュール MGMT0 ポートと，システムコンソールを LAN ケーブルで接続してください。マネジメントモジュールが 2 台搭載されている場合は, MSR ランプが緑色に点灯している側のマネジメントモジュールに接続してください。

図 1-2 システムコンソールとマネジメントモジュールの接続（LAN ケーブル）



重要

- マネジメントモジュールのネットワーク接続時，システム装置内のマネジメントモジュール，またはその他のモジュールと重複する IP アドレスを割り当てた機器がネットワーク上に存在する場合，システム装置に

障害が発生します。マネジメントモジュールのネットワークへの接続は，システム装置のネットワーク設定が完了してから行ってください。

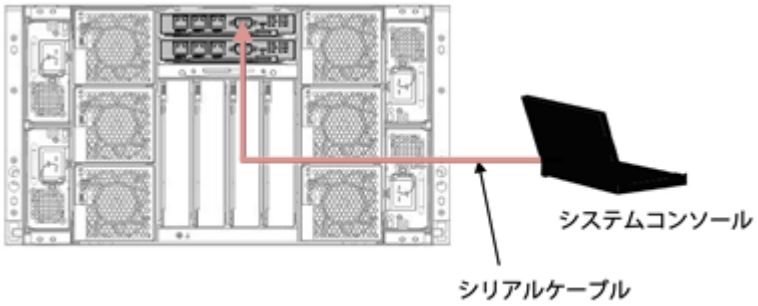
- HVM モードで使用する場合は，外部 LAN スイッチが必要です。詳細は「*BladeSymphony BS500 サーバブレードセットアップガイド*」を参照してください。

参考 システムコンソール用 LAN ポートは，ストレートケーブル，クロスケーブルのどちらでも使用できます。通信速度は，10/100/1000Mbps 自動選択となります。

(2) シリアルケーブルでの接続

システム装置背面のマネジメントモジュールシリアルポートと，システムコンソールを RS-232C クロスケーブルで接続してください。マネジメントモジュールが 2 台搭載されている場合は，MSR ランプが緑色に点灯している側のマネジメントモジュールに接続してください。

図 1-3 システムコンソールとマネジメントモジュールの接続（シリアルケーブル）



参考 システムコンソール用シリアルポートには，RS-232C クロスケーブル（D-SUB9 ピンメスーメス仕様）を使用してください。通信速度の工場出荷時設定は，9600bps となります。

1.3 機能一覧

マネジメントモジュールが提供する主な機能の一覧を次に示します。

詳細は項目名を参照してください。

表 1-4 主な機能一覧

大項目	小項目	Web コンソール	CLI コンソール	LCD タッチコンソール
2.1 ユーザ管理	2.1.2 アカウントの設定	○	○	－
	2.1.3 パスワード有効期限の設定	○	○	－
	2.1.5 ロールの設定	○	○	－
	2.1.6 LCD タッチコンソールの認証について	○ クリアのみ	○	○
2.2 時刻	2.2.1 マネジメントモジュールの時刻設定	○	○	○
	2.2.2 NTP サーバ連携	○	－	－
2.3 ネットワーク	2.3.3 内部ネットワーク	○	－	－
	2.3.4 スイッチモジュールの管理用インタフェース接続	○	○	－

大項目	小項目		Web コンソール	CLI コンソール	LCD タッチコンソール
	2.3.5 接続方式の設定	(1) MGMT1 からの管理用インタフェースへの接続	−	○	−
		(2) Tag-VLAN を使用した管理用インタフェースへの接続	−	○	−
	2.3.6 IP アドレスの設定	マネジメントモジュール	○ ※1	○ ※1	○
		サーバブレード	○ ※1	○ ※1	−
		スイッチモジュール	○	○	−
	2.3.8 Link Fault Tolerance(LFT)		○	−	−
2.4 セキュリティ	2.4.2 セキュリティ強度設定		○	○	−
	2.4.5 TLS/SSL バージョン設定機能		○	○	−
	2.4.6 マネジメントモジュールが提供するサービスの IP アドレス制限設定		○ ※1	○ ※1	○
	2.4.7 認証情報暗号化設定		−	○	−
2.5 システム装置設定	2.5.1 シャーシ ID 設定		○	○	−
	2.5.2 言語設定		○	○	−
2.6 電源制御	2.6.2 システム装置の電源を切る		○	○	○
	2.6.3 サーバブレードの電源を操作する		○	○	−
	2.6.4 スイッチモジュールの電源を操作する		○	−	−
	2.6.5 電源復旧時のサーバブレード動作設定		○	−	−
2.7 サーバブレードの遠隔操作	2.7.1 リモートコンソールによる操作		○	−	−
	2.7.2 OS コンソールによる操作		−	○	−
2.8 識別 LED(LID)の操作	フロントパネル		○	○	○
	マネジメントモジュール		○	○	○
	サーバブレード		○	○	○
	スイッチモジュール		○	○	○
2.9 装置内の各モジュールの設定	2.9.2 サーバブレード(BMC 設定)		○	○	−
	2.9.3 サーバブレード(UEFI 設定)		○	−	−
	2.9.4 Hitachi LAN スイッチモジュールの設定		○	−	−
	Brocade 8Gb ファイバチャネルスイッチモジュール, Brocade 8/16Gb ファイバチャネルスイッチモジュールおよび Brocade 16Gb ファイバチャネルスイッチモジュールの Web コンソールへのリンク		○	−	−
	スイッチモジュールの CLI コンソールへのリンク		−	○	−
2.10 本装置における WWN，MAC アドレスについて	2.10.3 Basic モードでの WWN，MAC アドレスの選択		○	○	−
	2.10.6 additional WWN，additional MAC アドレスの初期化		○	−	−
	2.10.7 WWN，MAC アドレスの確認方法		○	−	−
	2.10.8 additional WWN，additional MAC アドレスの変更ログ		○	○	−

大項目	小項目	Web コンソール	CLI コンソール	LCD タッチコンソール
2.11 ホスト情報の表示		○	−	−
2.12 JP1/ServerConductor/Blade Server Manager 連携	2.12.1 通知先 BSM の設定	○	−	−
2.13 HCSM 連携	2.13.1 HCSM からのディスカバリについて	○	○	−
	2.13.2 HCSM 連携のオプション設定	○	○	−
2.14 N+M コールドスタンバイ	2.14.8 Pre-configure 実行契機	○	−	−
	2.14.11(2) N+M コールドスタンバイ支援機能の有効化	○	−	−
	2.14.11(6) N+M 切り替えテスト実行	○	−	−
	2.14.14 N+M コールドスタンバイの UPS 接続設定	○	−	−
2.15 HA モニタ連携	2.15.2 系切り替え構成の設定方法	○	−	−
2.17 RADIUS 認証	2.17.4 マネジメントモジュールへの設定	○	−	−
	2.17.5 RADIUS サーバ接続確認	○	−	−
2.19 HVM 連携	2.19.1 HVM 初期設定	○	−	−
	2.19.2 HVM ファームウェアの選択	○	−	−
	2.19.3 仮想 WWN の確認	○	−	−
	2.19.4 仮想 MAC アドレスの確認	○	−	−
	2.19.5 電源の投入	○	−	−
	2.19.6 LPAR 作成	○	−	−
	2.19.7 HVM 構成情報の保存	○	−	−
	2.19.8 LPAR への USB 割り当ての設定	○	−	−
	2.19.9 LPAR のブートオーダ設定	○	−	−
	2.19.10 LPAR の Activate	○	−	−
	2.19.11 リモートコンソールの呼び出し	○	−	−
	2.19.12 LPAR の Reactivate	○	−	−
	2.19.13 LPAR の Deactivate	○	−	−
	2.19.14 LPAR 設定の変更	○	−	−
	2.19.15 LPAR の削除	○	−	−
	2.19.16 HVM の再起動	○	−	−
	2.19.17 HVM のシャットダウン	○	−	−
	2.19.18 HVM 設定のバックアップ	○	−	−
	2.19.19 HVM 設定のリストア	○	−	−
	2.19.20 HVM 設定の初期化	○	−	−
	2.19.21 HVM のモデルアップ	○	−	−
	2.19.22 HVM ファームウェアのアップデート	○	−	−
	2.19.23 HVM ファームウェアのアンインストール	○	−	−
2.20 省電力機能	2.20.2 設備保護電力制御機能	○	−	−
	2.20.3 運用時電力制御機能	○	−	−
	2.20.4 サーバブレードに対する電力制御の無効設定	○	−	−
	2.20.6 電力値のモニタリング表示	○	−	−

大項目	小項目		Web コンソール	CLI コンソール	LCD タッチコンソール
	2.20.7 電源容量超過時のサーバブレード強制電源 OFF 順序設定		○	－	－
	2.20.8 電源モジュール最適制御機能		○	○	－
2.21 DCMI 機能	2.21.3 DCMI モードの設定方法		○	○	－
2.22 静音モード	2.22.1 静音モード機能概要		○	－	－
2.23 SNMP 機能	2.23.3 SNMP 機能の設定手順		○	○	－
2.24 E-mail 通報機能	2.24.4 E-mail 通報機能の設定手順		○	○	－
	2.24.5 手動契機通報(現状通報)		○	○	－
2.26 USB ポートの無効化機能			○	○	－
2.27 インポート機能	2.27.2 インポート実施方法		○	－	○
2.28 ログ	システムイベントログ		○	○	－
	MAR ログ		○	○	－
	2.28.3 操作ログ		○	－	－
	環境ログ		○	○	－
	2.28.2 ダンプログ		○	○	○
2.29 ファームウェア	2.29.2 マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート		○	○	○
	2.29.3 サーバブレードファームウェアのアップデート		○	○	○
2.30 設定の保存と復元	2.30.2 マネジメントモジュール設定	(1) 保存	○	－	－
		(2) 復元	○	－	－
	2.30.3 Hitachi ファイバチャネル拡張カード設定	(1) 保存	－	○	－
	2.30.4 HVM 設定	(1) 保存	○	－	－
		(2) 復元	○	－	－

（凡例）

○：操作可能　－：操作不可

※1

IPv6 アドレスの設定も可能です。

2

機能詳細

この章では，マネジメントモジュールの機能について説明します。

- 2.1 ユーザ管理
- 2.2 時刻
- 2.3 ネットワーク
- 2.4 セキュリティ
- 2.5 システム装置設定
- 2.6 電源制御
- 2.7 サーバブレードの遠隔操作
- 2.8 識別 LED(LID)の操作
- 2.9 装置内の各モジュールの設定
- 2.10 本装置における WWN，MAC アドレスについて
- 2.11 ホスト情報の表示
- 2.12 JP1/ServerConductor/Blade Server Manager 連携
- 2.13 HCSM 連携
- 2.14 N+M コールドスタンバイ
- 2.15 HA モニタ連携
- 2.16 LDAP 連携
- 2.17 RADIUS 認証
- 2.18 Web コンソールにおけるデジタル証明書の利用

- 2.19 HVM 連携
- 2.20 省電力機能
- 2.21 DCMI 機能
- 2.22 静音モード機能
- 2.23 SNMP 機能
- 2.24 E-mail 通報機能
- 2.25 バナー機能
- 2.26 USB ポートの無効化機能
- 2.27 インポート機能
- 2.28 ログ
- 2.29 ファームウェア
- 2.30 設定の保存と復元

2.1 ユーザ管理

マネジメントモジュールのユーザ管理について説明します。

2.1.1 アカウントの概要

マネジメントモジュールのコンソール機能では，次の用途にアカウントが必要となります。

(1) コンソールへのログイン

Web コンソール，CLI コンソールにログインする際，各アカウントに対応したパスワードの入力が必要であり，不正なログインを防止します。アカウントを複数作成し，担当者によって使い分けることが可能です。

(2) FTP プロトコルを使用したファイルの送受信

マネジメントモジュールでは，FTP プロトコルにより，ユーザディレクトリに対するファイルの送信および受信を行うことができます。

ファイル送受信の機能を利用するには，アカウントとパスワードの入力が必要となります。

参考 LCD タッチコンソールへのログインの際は，アカウントは使用しません。不正なログインを防止するためには暗証番号を設定することができます。暗証番号については「2.1.6 LCD タッチコンソールの認証について」を参照してください。

2.1.2 アカウントの設定

アカウントは，マネジメントモジュールのコンソールから作成，変更，削除することができます。

アカウントは最大 16 個登録することができます。

アカウントを新規に作成する場合の設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

マネジメントモジュールには，工場出荷時にデフォルトで次のアカウントが登録されています。

表 2-1 工場出荷時のデフォルト値

項目	内容
ユーザ名	administrator
状態	有効
ロール	Administrators
言語	システム設定に従う
CLI コンソールのプロンプト	「シャーシ ID(マネジメントモジュールのスロット番号)$」
セッションタイムアウト時間	10 分
パスワード	password

重要

- 次のアカウントはシステムで予約されているため使用できません。
  Recovery で始まるアカウント / ResetPassword で始まるアカウント / root / bin / daemon / adm / lp / sync / shutdown / halt / mail / news / uucp / operator / games / gopher / ftp / sshd / nobody
- アカウントに使用できる文字は下記の範囲です。
  文字長：1～31 文字

使用可能文字（先頭）：[A-Z] [a-z]

使用可能文字（二文字目以降）：[A-Z] [a-z] [0-9]，"-"（ハイフン），"_"（アンダースコア），"."（ピリオド）

参考 セキュリティ上，システム装置の初期設定時に，新規のアカウントを作成して administrator アカウントを削除するか，administrator アカウントのパスワードを変更することを強く推奨します。

表 2-2 Web コンソールでの操作方法

項目	画面
アカウントの表示，設定	Administration タブ → ユーザとロール

表 2-3 CLI コンソールでの操作方法

項目	コマンド
アカウントの表示	show user account
アカウントの追加	add user account
アカウントの変更	modify user account
アカウントの削除	delete user account
アカウントのパスワード変更	change-password user account

重要 SMP 構成のサーバブレードに権限を設定する場合，Web コンソール上で SMP を構成するすべてのサーバブレードを選択してください。

2.1.3 パスワード有効期限の設定

マネジメントモジュールの Web コンソールおよび CLI コンソールにログインする際のパスワードに，有効期限を設けることができます。

マネジメントモジュールにパスワードを有効と見なす期間（日数）を設定することで，パスワード有効期限の管理ができます。

アカウントの新規作成やパスワードの変更操作を行なうと，その操作を行なったアカウントのパスワードに対し，有効期限が再設定されます。

有効期限は，（操作を行なった日）＋（有効と見なされる期間） で設定され，残り日数が「0 日」まで有効です。

参考 パスワード有効期間の残り日数が「0 日」となっている場合，その当日（システム時刻が翌日の日付になるまで）の間，パスワードは有効と見なされます。

パスワード有効期限の管理に関する表示・設定にはアカウント権限が必要です。

アカウントのパスワードが有効期限を超過した場合の動作は，次のどちらかを設定できます。

- パスワードの更新を要求する
- ログインを許可しない

「パスワードの更新を要求する」設定とした場合，マネジメントモジュールは，期限切れのパスワードを用いたコンソールへのログイン要求に対し，パスワードを更新するための画面を表示してログインを許可し，そのアカウント使用者自身がパスワードを変更することができます。

「ログインを許可しない」設定とした場合，マネジメントモジュールのコンソールにログインすることができなくなり，期限切れのパスワードの変更は，管理者が行なう必要があります。このとき「期限切れのパスワードのユーザによる変更」を設定することで，新たにログイン要求があった際に，

1 回だけパスワードを更新するための画面を表示してログインを許可し，そのアカウント使用者自身がパスワードを変更することができます。

アカウント権限を持ったアカウントのパスワードが有効期限を超過した場合は，設定に関わらず「パスワードの更新を要求する」動作となります。

この機能の対象はマネジメントモジュールに登録されたアカウントです。LDAP 連携を行なう場合は，LDAP ディレクトリ上のユーザアカウントに対してはパスワード有効期限管理を行いません。

工場出荷時の初期値では，パスワード有効期限の管理は無効となっています。

表 2-4 パスワード有効期限管理の工場出荷時の設定

項目	設定値
有効期限の管理	しない
パスワード有効期間	無期限
期限切れパスワードのユーザによる変更	許可しない

参考 パスワード有効期限を管理する場合，パスワード有効期間には 1～365(日)の範囲で値を設定してください。

表 2-5 Web コンソールでの操作方法

項目	画面
パスワード有効期限の管理	Administration タブ→ユーザとロール→パスワードポリシータブ
アカウント毎の有効期間の表示，期限切れパスワード変更方法の表示，設定	Administration タブ→ユーザとロール→ユーザアカウントタブ

表 2-6 CLI コンソールでの操作方法

項目	コマンド
パスワード有効期限管理の表示	show user password policy
パスワード有効期限管理の設定	set user password policy
アカウント毎の有効期間，期限切れパスワード変更方法の表示	show user account
アカウント毎の期限切れパスワード変更方法の設定	modify user account

2.1.4 ロールの概要

マネジメントモジュールのコンソール機能では，お客様のユーザ管理にあわせて，各権限の許可・不許可を設定することで，権限をカスタマイズしたロールが定義できます。ロールに設定可能な権限の一覧を次に示します。

表 2-7 権限の一覧

権限名称	説明
サーバブレード	サーバブレードの操作，設定が可能な権限です。サーバブレードスロットごとに権限が分かれています。リモートコンソールの操作，設定が可能か否かを選択できます。
スイッチモジュール	スイッチモジュールの操作，設定が可能な権限です。スイッチモジュールスロットごとに権限が分かれています。
ネットワーク	ネットワークの設定が可能な権限です。
シャーシ	サーバシャーシの操作，設定が可能な権限です。

権限名称	説明
アカウント	アカウント，ロールの追加や削除が可能な権限です。

また，上記設定とは独立して，ロールに readonly の属性を付与することができます。readonly の属性を付与した場合，権限を持つ項目のうち，内容の参照のみが行えます。設定や操作は行えません。

システム装置には，次の組み込みロールが用意されています。このロールは変更および削除することができません。

表 2-8 組み込みロール

ロール名称	説明
Administrators	すべての権限が付与されたロールです。

参考 SMP 構成のサーバブレードへ権限を設定する場合は，構成する全サーバブレードに設定してください。

2.1.5 ロールの設定

ロールは，マネジメントモジュールのコンソールから作成，変更，削除することができます。

ロールは最大 16 個登録することができます。

ただし，組み込みロールは 16 個の中には含まれません。

表 2-9 Web コンソールでの操作方法

項目	画面
ロールの表示，設定	Administration タブ → ユーザとロール → Action → ロールの表示と設定

表 2-10 CLI コンソールでの操作方法

項目	コマンド
ロールの表示	show user role
ロールの追加	add user role
ロールの変更	modify user role
ロールの削除	delete user role

2.1.6 LCD タッチコンソールの認証について

LCD タッチコンソールではアカウントによる認証は行いません。LCD タッチコンソールの不正利用を防止するために，暗証番号を設定することができます。

また，LCD タッチコンソール機能自体を無効化することができます。

(1) 暗証番号設定

暗証番号設定はシステム装置に対して実施します。そのため異なる LCD タッチコンソールでも入力する暗証番号は共通です。

暗証番号を使用する設定とした場合, 暗証番号を入力しないと LCD タッチコンソールを使用できません。

暗証番号は数字 4 文字で設定します。工場出荷時の初期値は暗証番号を使用しない設定となっています。暗証番号の文字列が画面に表示されることは無いため，お客様ご自身で暗証番号の内容を大切に保管してください。暗証番号を忘れてしまった場合，Web コンソールから暗証番号の初期化を実施することができます。暗証番号の初期化を実施した場合，暗証番号を使用しない設定に戻ります。

表 2-11 Web コンソールでの操作方法

項目	画面
暗証番号の初期化	Administration タブ → ユーザとロール → Action → LCD PIN 初期化

表 2-12 LCD タッチコンソールでの操作方法

項目	画面
暗証番号の設定	システム構築 → 暗証番号設定

(2) 無効化設定

無効化設定はシステム装置に対して実施します。LCD タッチコンソール機能自体を無効化する設定です。

LCD タッチコンソールの無効化設定をした場合，システム装置に LCD タッチコンソールを挿入しても，LCD タッチコンソールの操作はできません。

工場出荷時の初期値は有効設定となっています。

設定の変更は CLI コンソールから実施することができます。

表 2-13 CLI コンソールでの操作方法

項目	コマンド
LCD タッチコンソールの有効無効設定の表示	show lcd setting
LCD タッチコンソールの有効無効設定の設定	set lcd validity

2.2 時刻

システム装置の時刻設定について説明します。

2.2.1 マネジメントモジュールの時刻設定

マネジメントモジュールには，日付，時刻，タイムゾーン，夏時間の設定が可能です。

システム装置の運用開始前に，正確な時刻に合わせてください。

表 2-14 Web コンソールでの操作方法

項目	画面
時刻関連情報の表示，設定	Administration タブ → 時刻設定

表 2-15 CLI コンソールでの操作方法

項目	コマンド
時刻関連情報の表示	show time local show time timezone

項目	コマンド
時刻関連情報の設定	set time local set time timezone

表 2-16 LCD タッチコンソールでの操作方法

項目	画面
時刻関連情報の表示，設定	システム構築 → 時刻設定

2.2.2 NTP サーバ連携

システム装置外部に NTP(Network Time Protocol)サーバを設置することで，マネジメントモジュールの時刻を NTP サーバと同期させることができます。NTP サーバは最大 4 台設置でき，複数の NTP サーバを設置した場合はいずれかの NTP サーバが故障した場合でも時刻を同期し続けることができます。

NTP による時刻同期は，システム装置の起動直後に実施し，その後 30 分おきに実施します。また，マネジメントモジュールのコンソール操作で，時刻を強制的に同期させることが可能です。システム装置の工場出荷時設定では，NTP サーバ連携機能は無効となっています。

図 2-1 NTP サーバの連携イメージ

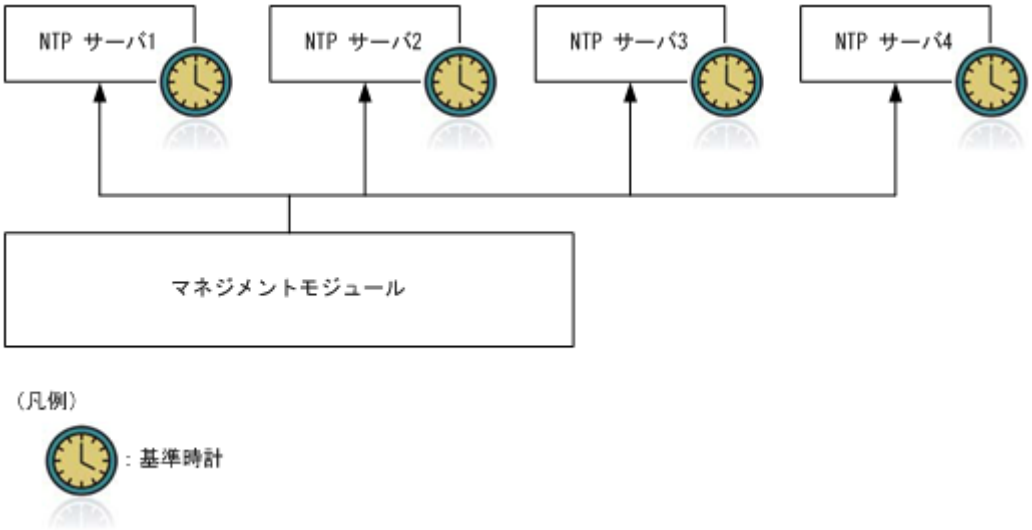


表 2-17 Web コンソールでの操作方法

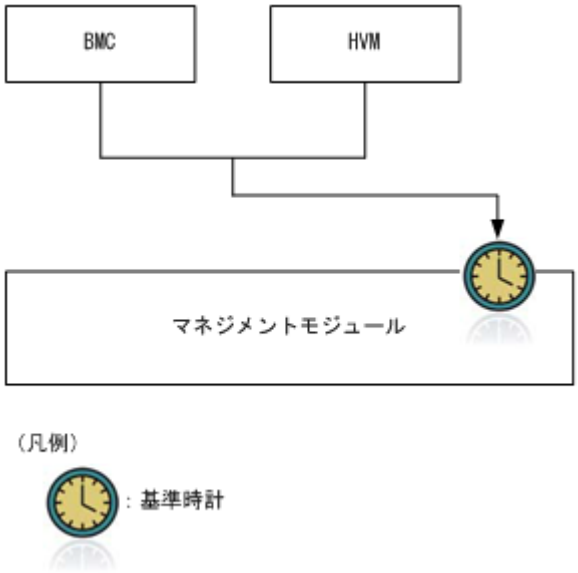
項目	画面
NTP サーバ関連情報の表示，設定	Administration タブ → 時刻設定

2.2.3 システム装置の時刻管理方式

マネジメントモジュールは，NTP サーバとなり，システム装置内の各モジュールに対して時刻同期をすることができます。時刻同期をすることが可能なモジュールは次のとおりです。

- BMC
- HVM

図 2-2 マネジメントモジュールの時刻同期イメージ



なお，マネジメントモジュールから時刻同期をするには，それぞれ次の設定を行う必要があります。

- BMC
  BMC の時刻設定で，「NTP を使用してマネジメントモジュールに時刻を合わせる」を選択する。
  BMC の時刻同期は，起動直後に実施し，その後 15 分おきに実施する。
- HVM
  HVM コンソールで，マネジメントモジュールによる時刻合わせを行うように設定する。
  HVM の時刻同期は，起動直後に実施し，その後 15 分おきに実施する。

重要 BS520X サーバブレード B1/B2 では「NTP を使用してマネジメントモジュールに時刻を合わせる」だけが設定できます。

参考

- システム装置の工場出荷時設定では，BMC の時刻設定は「マネジメントモジュールから同期」となっています。本設定のまま使用することを推奨します。
- マネジメントモジュールから時刻同期をする場合，マネジメントモジュールの時刻を NTP サーバと同期させることを推奨します。
- HVM コンソールについての詳細は，「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

表 2-18 Web コンソールでの操作方法

項目	画面
BMC の時刻設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → BMC タブ

2.3 ネットワーク

システム装置のネットワークについて説明します。

2.3.1 各モジュールの管理用インタフェースで使用可能な機能一覧

システム装置に搭載されるマネジメントモジュール，サーバブレード，スイッチモジュールは，それぞれ管理用インタフェースを持っています。

各モジュールの管理用インタフェースにネットワーク接続すると，各モジュールのコンソール，また HCSM や SNMP などの管理ソフトウェアとの通信などが使用可能です。

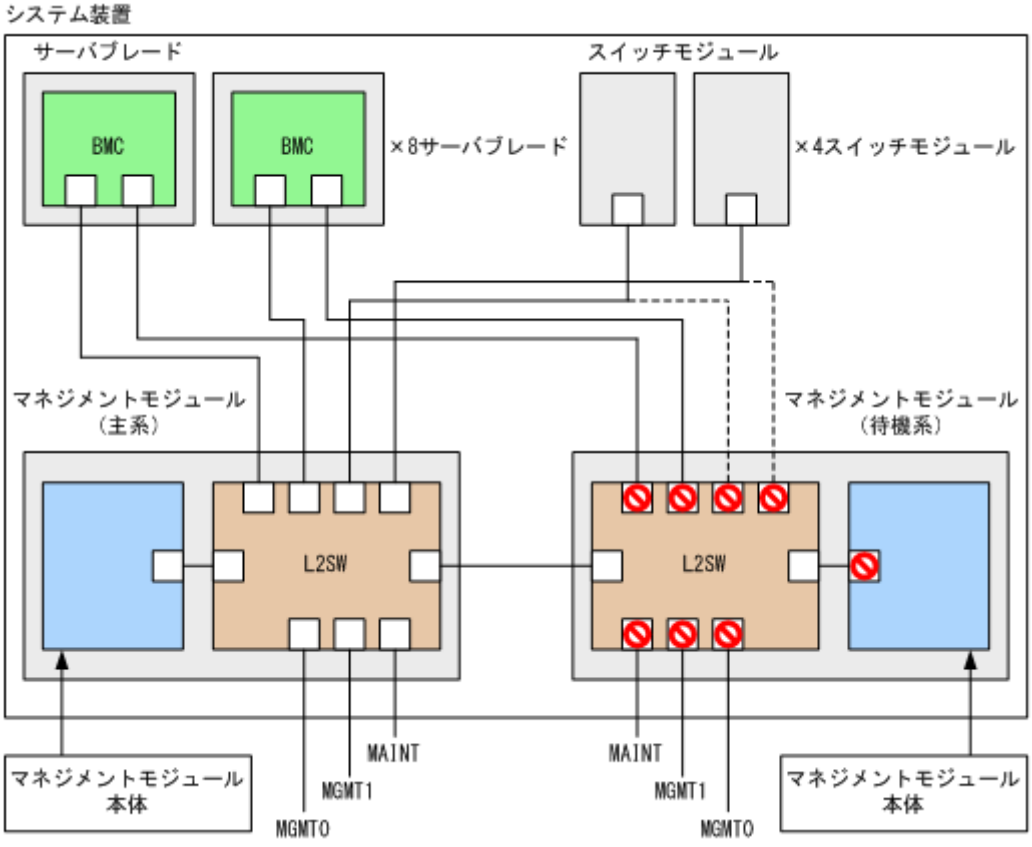
なお，マネジメントモジュールが二重化されているときは，マネジメントモジュールの管理用インタフェースは主系側のインタフェースのみが有効となります。

2.3.2 管理ネットワーク

マネジメントモジュールは L2SW を内蔵しており，各モジュールの管理用インタフェースは装置内で接続されています。マネジメントモジュールには外部出力ポート(MGMT0，MGMT1)があり，外部出力ポートにケーブル接続することで，各モジュールの管理用インタフェースに接続することができます。

以降，本ネットワークのことを管理ネットワークと呼びます。

管理ネットワークの概略図は次のとおりです。



参考

- MAINT ポートは保守専用ポートです。お客様は使用できません。保守作業の支障となりますので，ケーブル接続はしないでください。
- 待機系マネジメントモジュールのポートは通常クローズされており，マネジメントモジュールの障害時や Link Fault Torelance 機能の切り替わり時にオープンされます。

2.3.3 内部ネットワーク

システム装置は，管理ネットワークとは別に装置内部に内部ネットワークを保持し，次の用途に使用しています。

- マネジメントモジュール間の制御用通信
- マネジメントモジュールーサーバブレード間の制御用通信
- マネジメントモジュールースイッチモジュール間の制御用通信

内部ネットワーク用に，システム装置は 24bit マスクのネットワーク(サブネットマスクが 255.255.255.0 のネットワーク)を一つ使用します。システム装置の工場出荷時は，192.168.253.0/255.255.255.0 が設定されています。内部ネットワークで使用している IP アドレスは，システム装置外では使用できません。192.168.253.0/255.255.255.0 で指定されるネットワークの IP アドレスをシステム装置外で使用したい場合，内部ネットワークの設定を変更してください。

重要

- 内部ネットワークの変更を行うと，マネジメントモジュールがリスタートします。
- サーバブレード稼働中の内部ネットワーク変更は実施しないでください。
  設定変更した場合，マネジメントモジュールがリスタートするため再起動中に発生した障害イベントを検出できない場合があります。

参考 192.168.253.0/255.255.255.0 で指定されるネットワークの IP アドレスをシステム装置外で使用しない場合は，内部ネットワークの設定変更は不要です。

表 2-19 Web コンソールでの操作方法

項目	画面
内部ネットワークの表示，設定	Resources タブ → Systems → ネットワーク管理 → 内部 LAN

2.3.4 スイッチモジュールの管理用インタフェース接続

スイッチモジュールの管理用インタフェースへの接続方法は,「マネジメントモジュールコンソール経由で接続する」,「管理 LAN ポートから直接接続する」,「スイッチモジュール外部ポートに接続する」の 3 種類から選択することができ，マネジメントモジュールのコンソールから設定可能です。それぞれの接続方法によって使用可能な機能は次のとおりです。

マネジメントモジュールコンソール経由で接続する

(a)CLI コンソールの change console コマンドで, スイッチモジュールのテキストコンソールに接続可能。(Brocade 10Gb DCB スイッチモジュール，Brocade 8/16Gb ファイバチャネルスイッチモジュールおよび Brocade 16Gb ファイバチャネルスイッチモジュールでは, 管理 LAN ポートから直接接続するを選択していても，管理 LAN ポートに 0.0.0.0 を設定していない場合であれば本機能を使用可能です)

(b)マネジメントモジュールの Web コンソールから，LAN スイッチモジュールの設定および表示が可能。(Hitachi 1Gb LAN スイッチモジュール(20 ポート, 40 ポート), Hitachi 1/10Gb LAN スイッチモジュールのみ)

管理 LAN ポートから直接接続する

(c)装置外部のクライアントから，スイッチモジュールのテキストコンソール，Web コンソールに接続可能。

(d)管理 LAN ポート経由で，スイッチモジュールの SNMP などの機能を使用可能。

(e)マネジメントモジュールの Web コンソールからスイッチモジュールの Web コンソールにリンク可能。(Brocade 8Gb ファイバチャネルスイッチモジュール，Brocade 8/16Gb ファイバチャネルスイッチモジュールおよび Brocade 16Gb ファイバチャネルスイッチモジュールのみ)

スイッチモジュール外部ポートに接続する

(f)外部ポート経由で，スイッチモジュールの SNMP などの機能を使用可能。(Brocade 8Gb ファイバチャネルスイッチモジュールのみ)

本装置でサポートしているスイッチモジュールには次の 6 種類があります。

- Hitachi 1Gb LAN スイッチモジュール(20 ポート，40 ポート)
- Hitachi 1/10Gb LAN スイッチモジュール
- Brocade 10Gb DCB スイッチモジュール
- Brocade 8Gb ファイバチャネルスイッチモジュール
- Brocade 8/16Gb ファイバチャネルスイッチモジュール
- Brocade 16Gb ファイバチャネルスイッチモジュール

それぞれのスイッチモジュールの管理用インタフェース接続方法とそのサポート機能の差異を次に示します。

スイッチモジュール	接続方法	(a)	(b)	(c)	(d)	(e)	(f)
Hitachi 1Gb LAN スイッチモジュール(20 ポート，40 ポート)	マネジメントモジュールコンソール経由で接続する	○	○	×	×	×	×
	管理 LAN ポートから直接接続する	×	×	○	○	×	×
	スイッチモジュール外部ポートに接続する	×	×	×	×	×	×
Hitachi 1/10Gb LAN スイッチモジュール	マネジメントモジュールコンソール経由で接続する	○	○	×	×	×	×
	管理 LAN ポートから直接接続する	×	×	○	○	×	×
	スイッチモジュール外部ポートに接続する	×	×	×	×	×	×
Brocade 10Gb DCB スイッチモジュール	マネジメントモジュールコンソール経由で接続する（※1）	○	×	×	×	×	×
	管理 LAN ポートから直接接続する	○	×	○	○	×	×
	スイッチモジュール外部ポートに接続する	×	×	×	×	×	×
Brocade 8Gb ファイバチャネルスイッチモジュール	マネジメントモジュールコンソール経由で接続する	○	×	×	×	×	×

スイッチモジュール	接続方法	(a)	(b)	(c)	(d)	(e)	(f)
	管理 LAN ポートから直接接続する	×	×	○	○	○	×
	スイッチモジュール外部ポートに接続する	×	×	×	×	×	○
Brocade 8/16Gb ファイバチャネルスイッチモジュール Brocade 16Gb ファイバチャネルスイッチモジュール	マネジメントモジュールコンソール経由で接続する	○	×	×	×	×	×
	管理 LAN ポートから直接接続する	○	×	○	○	○	×
	スイッチモジュール外部ポートに接続する	×	×	×	×	×	×

(※1)マネジメントモジュールの Web コンソールからでは設定できず，マネジメントモジュールの CLI コンソールのみから設定可能です。

重要

- Hitachi 1Gb LAN スイッチモジュール(20 ポート，40 ポート)，Hitachi 1/10Gb LAN スイッチモジュールで，外部ポートを使用する場合は，「スイッチモジュール外部ポートに接続する」ではなく，「管理 LAN ポートから直接接続する」もしくは「マネジメントモジュールコンソール経由で接続する」を選択し，外部ポートにはスイッチモジュールのコンソールから IP アドレスを直接設定して使用してください。
- Brocade 10Gb DCB スイッチモジュール，Brocade 8/16Gb ファイバチャネルスイッチモジュールおよび Brocade 16Gb ファイバチャネルスイッチモジュールを使用して CLI コンソールの change console コマンドを使用する場合は，スイッチモジュールの IP アドレスを 0.0.0.0 以外に設定してください。
- Brocade 10Gb DCB スイッチモジュールを使用し，マネジメントモジュールの CLI コンソールから「マネジメントモジュールコンソール経由で接続する」を設定した後に，マネジメントモジュールの Web コンソールで設定値を確認すると，「管理 LAN ポートから直接接続する」が表示されます。その際にマネジメントモジュールの Web コンソールから設定を変更せずに保存すると，「管理 LAN ポートから直接接続する」が設定されます。

表 2-20 Web コンソールでの操作方法

項目	画面
接続方法の表示，設定	Resources タブ → Systems → ネットワーク管理 → 管理 LAN

2.3.5 接続方式の設定

各モジュールの管理用インタフェースは，MGMT0 または MGMT1 から接続できます。

接続方式は次から選択してください。設定はモジュール単位で変更できます。

- MGMT0 から接続
  工場出荷時の設定です。
- MGMT1 から接続
  詳細は「(1) MGMT1 からの管理用インタフェースへの接続」を参照してください。
- Tag-VLAN による接続(MGMT0/MGMT1)
  詳細は「(2) Tag-VLAN を使用した管理用インタフェースへの接続」を参照してください。

重要 スイッチモジュールの管理用インタフェースは，内部ネットワークに割り当てないでください。MGMT0，MGMT1 いずれからも接続できなくなります。

接続方式の工場出荷時の設定は下表のとおりです。

表 2-21 接続方式の工場出荷時の設定

モジュール名	設定値	備考
マネジメントモジュール	MGMT0 から接続	－
サーバブレード	MGMT0 から接続	－
スイッチモジュール	MGMT0 から接続	ただし，管理用インタフェースが内部ネットワークに割り当てられているので，Brocade 10Gb DCB スイッチモジュール以外のスイッチモジュールは MGMT0 からは接続できません。

表 2-22 Web コンソールでの操作方法

項目	画面
接続方式，VLAN の表示	Resources タブ → Systems → ネットワーク管理 → 管理 LAN → VLAN タブ

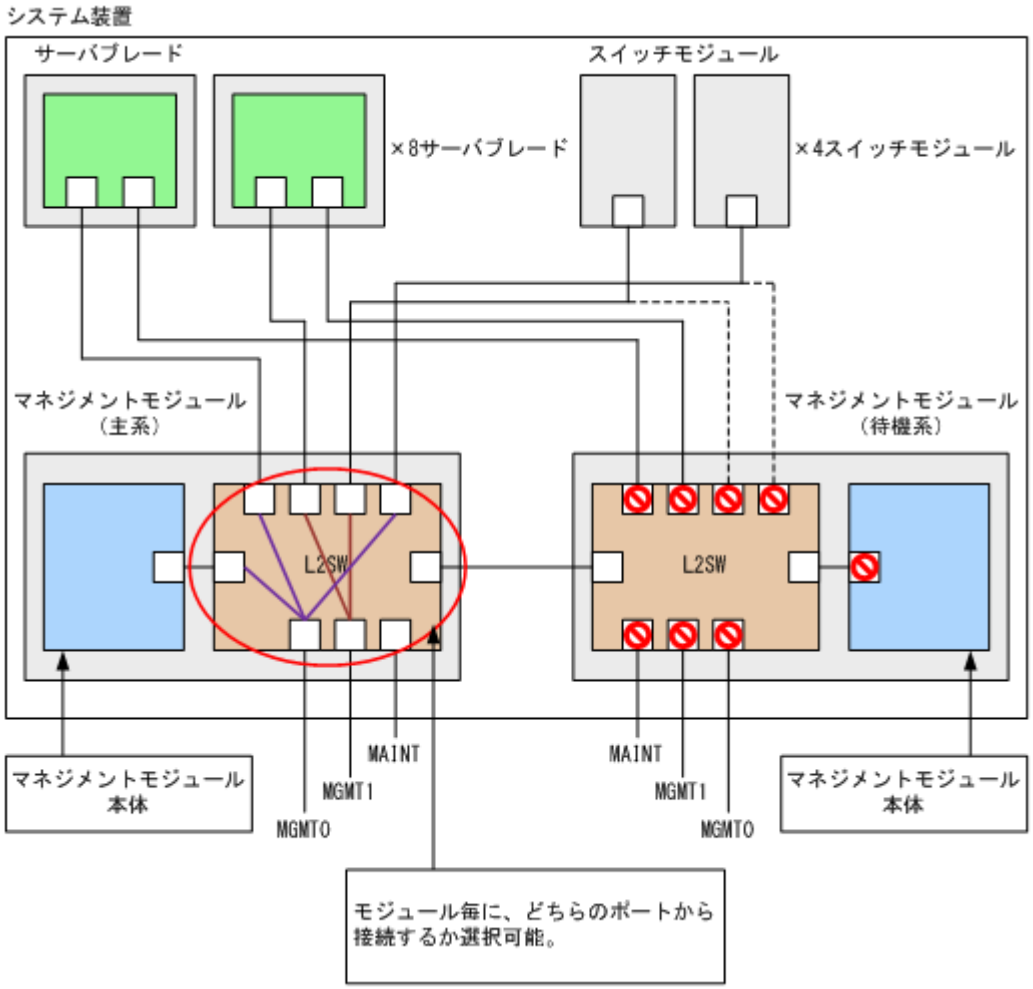
表 2-23 CLI コンソールでの操作方法

項目	コマンド
接続方式，VLAN の表示	show network vlan
接続方式，VLAN の設定	set network vlan
VLAN の削除	delete network vlan

(1) MGMT1 からの管理用インタフェースへの接続

システム装置は，管理ネットワークへの接続ポートとして MGMT0，MGMT1 を備えています。これを各モジュール単位でどちらから接続するかを選択できます。これにより，例えば次のような構成を組むことができます。

- マネジメントモジュールは MGMT0，サーバブレードとスイッチモジュールは MGMT1 から接続として，管理対象に応じてネットワークを明確に分離する。
- サーバブレード 0～3 は MGMT0，サーバブレード 4～7 は MGMT1 として，負荷を分散させる。



(2) Tag-VLAN を使用した管理用インタフェースへの接続

管理用インタフェースへ接続する場合，MGMT0，MGMT1 と対向スイッチの間で Tag-VLAN（IEEE802.1Q）を使用することができます。これにより，例えば次のような構成を組むことができます。

- サーバブレードごとに別の VLAN に所属させ，サーバブレードを使用するユーザがほかのサーバブレードと物理的に接続できないようにセキュリティを高める。
- モジュールごとに別の VLAN に所属させ，管理対象に応じてネットワークを明確に分割する。（MGMT0，MGMT1 の分割だけでは足りない場合など）

VLAN は最大 13 個作成可能で，作成可能な VLAN ID は 2～4000 となります。作成した VLAN には MGMT0 か MGMT1 のどちらかを入れる必要があり，MGMT0 と MGMT1 を同一の VLAN に入れることはできません。

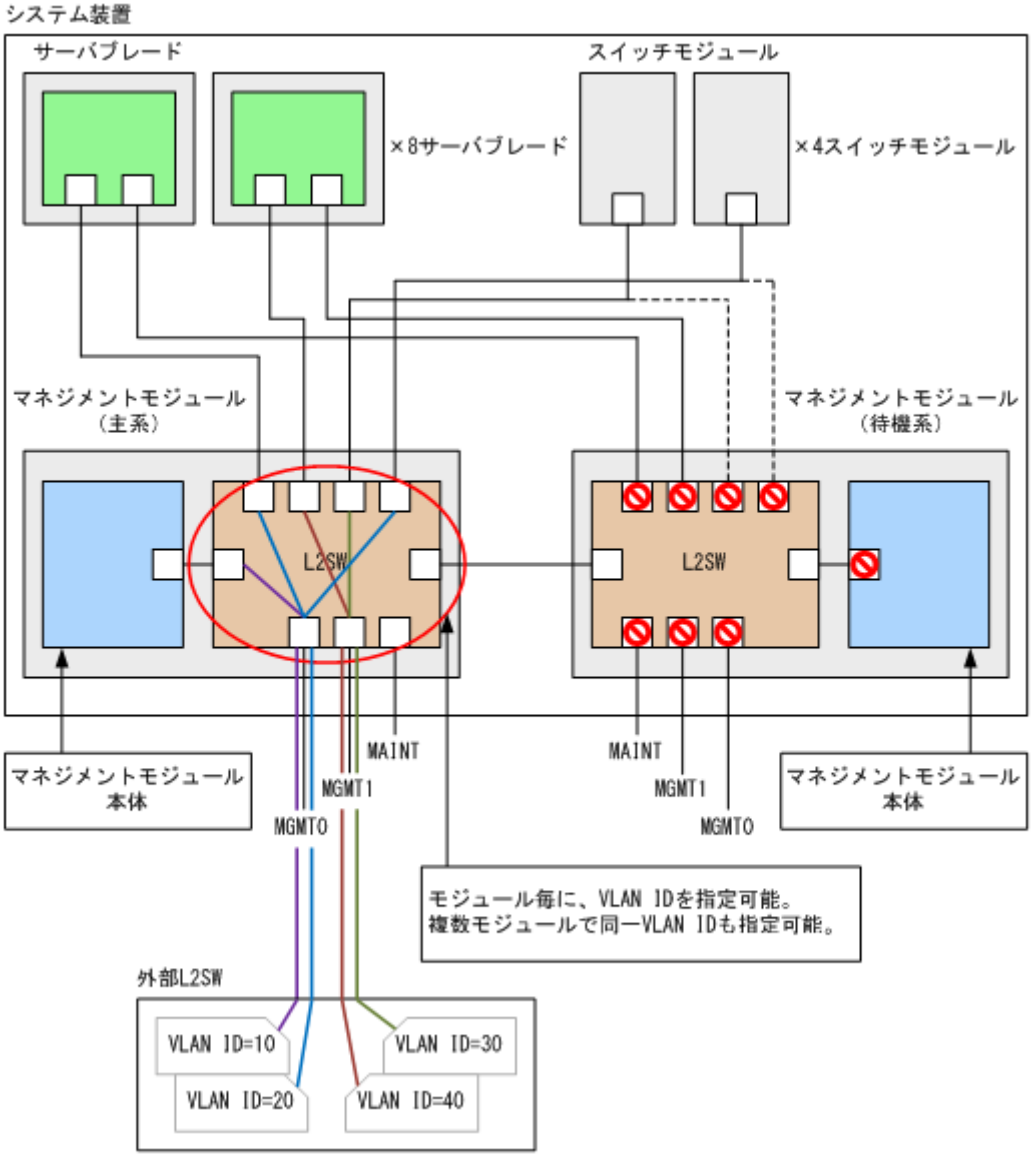
本機能と，MGMT1 からの管理用インタフェースへの接続機能は併用できます。

これにより，次のような構成を組むことができます。

- マネジメントモジュールとスイッチモジュールを MGMT0 から VLAN 無しで接続，サーバブレード 0～3 を MGMT0 から VLAN ID=10～13 で接続，サーバブレード 4～7 を MGMT1 から VLAN ID=20～23 で接続とし，用途ごとにネットワークを分けるとともに，負荷分散を行う。

重要 VLAN ID=1 と 4001～4094 は装置内部で使用するため，お客様は使用できません。

参考 本機能を使用する場合，対向スイッチも IEEE802.1Q VLAN をサポートしている必要があります。



2.3.6 IP アドレスの設定

各モジュールの管理用インタフェースは，マネジメントモジュールから設定することができます。

IPv6 ネットワークに対応している機能は，IPv4 アドレスの他に IPv6 アドレスを設定することができます。IP アドレスと記述している項目は，IPv4 アドレスあるいは IPv6 アドレスを示します。

(1) IP アドレスの工場出荷時設定

IP アドレスの工場出荷時の設定は次のとおりです。

表 2-24 IP アドレスの工場出荷時の設定

モジュール名	IP アドレス	サブネットマスク	デフォルトゲートウェイ
マネジメントモジュール	192.168.0.1	255.255.255.0	0.0.0.0
サーバブレード 0～7	0.0.0.0	0.0.0.0	0.0.0.0
スイッチモジュール 0	192.168.253.35	255.255.255.240	0.0.0.0

モジュール名	IP アドレス	サブネットマスク	デフォルトゲートウェイ
スイッチモジュール 1	192.168.253.36	255.255.255.240	0.0.0.0
スイッチモジュール 2	192.168.253.37	255.255.255.240	0.0.0.0
スイッチモジュール 3	192.168.253.38	255.255.255.240	0.0.0.0

重要

- Hitachi 1Gb LAN スイッチモジュール(20 ポート)または Hitachi 1/10Gb LAN スイッチモジュールのバージョンが「10.7.H」以前，Hitachi 1Gb LAN スイッチモジュール(40 ポート)のバージョンが「11.6」以前で，スイッチモジュールの初期アカウント（operator，パスワード無し）を削除した場合は，マネジメントモジュールのコンソールから，スイッチモジュールの認証情報（アカウント，パスワード，管理者パスワード）を設定してください。認証情報を設定しない場合，IP アドレスの設定に失敗します。
- Brocade 10Gb DCB スイッチモジュール，Brocade 8Gb ファイバチャネルスイッチモジュール，Brocade 8/16Gb ファイバチャネルスイッチモジュール，Brocade 16Gb ファイバチャネルスイッチモジュールの IP アドレスをスイッチモジュールのコンソールから変更しないでください。変更をした場合，変更直後は変更した IP アドレスが使用できますが，スイッチモジュールのリスタート，電源オフ/オンをすると，マネジメントモジュールのコンソールから設定した値で上書きされてしまいます。
- Hitachi 1Gb LAN スイッチモジュール(20，40 ポート)，Hitachi 1/10Gb LAN スイッチモジュールのデフォルトゲートウェイに 0.0.0.0 以外を指定した場合，インタフェース指定なしのデフォルトゲートウェイを全て削除した後に指定した値を追加します。したがって，VLAN にデフォルトゲートウェイを指定しておきたい場合は，VLAN ID 指定ありのデフォルトゲートウェイ設定としておく必要があります。また，マルチパス経路を指定したい場合は，デフォルトゲートウェイに 0.0.0.0 を指定しておき，LAN スイッチモジュールのコンソールに直接ログインして，デフォルトゲートウェイ設定を行う必要があります。
- Hitachi 1Gb LAN スイッチモジュール(20，40 ポート)，Hitachi 1/10Gb LAN スイッチモジュールのデフォルトゲートウェイを 0.0.0.0 以外に設定した後，デフォルトゲートウェイを 0.0.0.0 の設定に戻した場合，および，スイッチモジュールの接続種別を管理 LAN 以外に変更した場合は，マネジメントモジュールはデフォルトゲートウェイ設定を削除しませんので，LAN スイッチモジュールのコンソールに直接ログインして，デフォルトゲートウェイ設定の削除を行う必要があります。
- Brocade 10Gb DCB スイッチモジュールの Network OS が Ver.3.0.0 の場合，マネジメントモジュールからのデフォルトゲートウェイ設定は，DCB スイッチモジュールに反映されません。DCB スイッチモジュールにログインし，ip route コマンドを使って設定してください。設定方法については，「*BladeSymphony 10Gb DCB スイッチ Network OS 管理者ガイド*」を参照してください。なお，Network OS が Ver.2.0.1 の場合は，デフォルトゲートウェイの設定はできません。
- Hitachi 1Gb LAN スイッチモジュール(20，40 ポート)，Hitachi 1/10Gb LAN スイッチモジュールの場合，設定する IP アドレスを当該スイッチモジュールの他ポートで使用されている IP アドレスとは別のネットワークセグメントとしてください。同一ネットワークセグメントの IP アドレスを設定した場合，IP アドレスの設定に失敗します。

参考 SMP 構成のノンプライマリサーバブレードに，IPMI over LAN，SMASH-CLP，および WS-MAN を適用しない場合は，IP アドレスは出荷時設定の 0.0.0.0 を利用してください。

(2) IP アドレスの設定方法

各モジュールの IP アドレスは，次の方法で設定することができます。IPv6 ネットワークを使用する場合は，IPv4 アドレスの他に IPv6 アドレスを設定します。

表 2-25 Web コンソールでの操作方法

項目	画面
IPv4 アドレスの表示，設定	Resources タブ → Systems → ネットワーク管理 → 管理 LAN → IP アドレス(v4)タブ
IPv6 アドレスの表示，設定	Resources タブ → Systems → ネットワーク管理 → 管理 LAN → IP アドレス(v6)タブ

項目	画面
LAN スイッチモジュールの認証情報の設定，削除	Resources タブ → Modules → 全モジュール → スイッチモジュール → スイッチモジュール x

表 2-26 CLI コンソールでの操作方法

項目	コマンド
マネジメントモジュールの IPv4 アドレスの表示	show mgmt-module mgmt-lan
マネジメントモジュールの IPv4 アドレスの設定	set mgmt-module mgmt-lan
マネジメントモジュールの IPv6 アドレスの表示	show mgmt-module mgmt-v6 setting
マネジメントモジュールの IPv6 アドレスの設定	set mgmt-module mgmt-v6 address
サーバブレードの IPv4 アドレスの表示	show blade mgmt-lan
サーバブレードの IPv4 アドレスの設定	set blade mgmt-lan
サーバブレードの IPv6 アドレスの表示	show blade mgmt-v6 setting
サーバブレードの IPv6 アドレスの設定	set blade mgmt-v6 address
スイッチモジュールの IP アドレスの表示	show sw-module mgmt-lan
スイッチモジュールの IP アドレスの設定	set sw-module mgmt-lan
LAN スイッチモジュールの認証情報の設定	set sw-module lansw authentication
LAN スイッチモジュールの認証情報の削除	delete sw-module lansw authentication

表 2-27 LCD タッチコンソールでの操作方法

項目	画面
マネジメントモジュールの IPv4 アドレスの表示，設定	システム構築 → ネットワーク設定

LCD タッチコンソールで設定できるのは，IPv4 アドレスだけです。

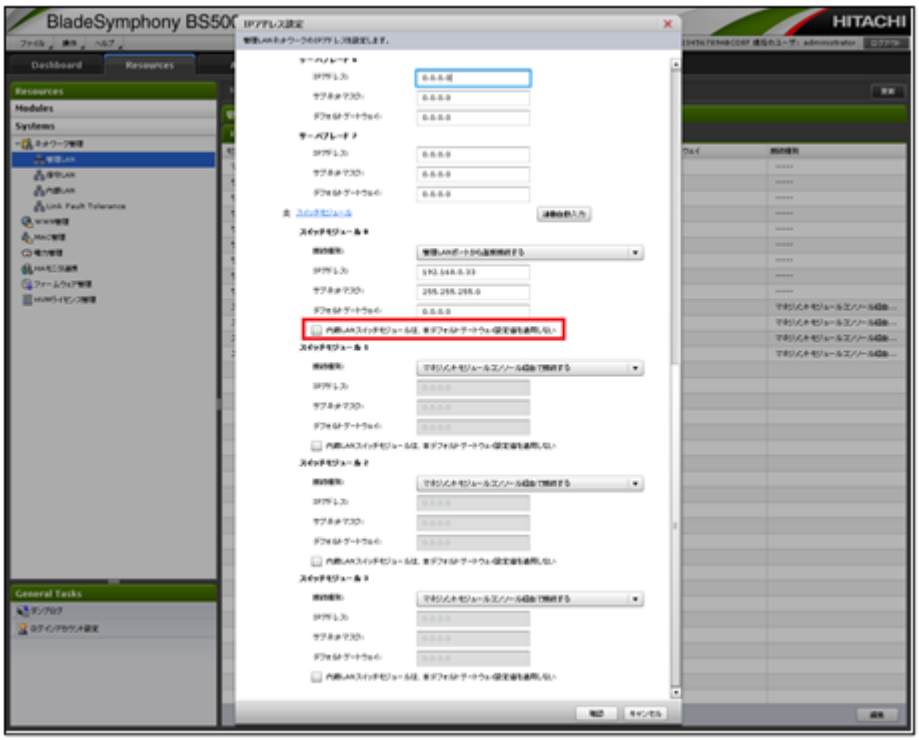
次に示す LAN スイッチモジュールの場合, LAN スイッチモジュールの認証情報の設定は不要です。

- Hitachi 1Gb LAN スイッチモジュール(20 ポート)でバージョン「10.7.K」以降の場合
- Hitachi 1/10Gb LAN スイッチモジュールでバージョン「10.7.K」以降の場合
- Hitachi 1Gb LAN スイッチモジュール(40 ポート)でバージョン「11.6.B」以降の場合

なお，2012 年 10 月以降に出荷したシステム装置は，認証情報の設定が不要なバージョンで出荷されています。

LAN スイッチモジュールのデフォルトゲートウェイ設定を適用しない場合，次の IP アドレス設定画面で[内蔵 LAN スイッチモジュールは，本デフォルトゲートウェイ設定値を適用しない]をチェックしてください。

適用する場合は，チェックを外してください。



重要

- [内蔵 LAN スイッチモジュールは，本デフォルトゲートウェイ設定値を適用しない]のチェックを外して LAN スイッチモジュールのデフォルトゲートウェイ設定を 0.0.0.0 にしても適用されませんので，LAN スイッチモジュールのコンソールに直接ログインして，デフォルトゲートウェイを設定してください。
- 出荷時のマネジメントモジュールのファームウェアバージョンバージョンが A0125 以前の場合，[内蔵 LAN スイッチモジュールは，本デフォルトゲートウェイ設定値を適用しない]のチェックがついています。マネジメントモジュールのファームウェアアップデートを行っても，この設定は変わりません。[内蔵 LAN スイッチモジュールは，本デフォルトゲートウェイ設定値を適用しない]のチェックを外さない場合は，LAN スイッチモジュールに直接ログインして，デフォルトゲートウェイを設定してください。

参考 [内蔵 LAN スイッチモジュールは，本デフォルトゲートウェイ設定値を適用しない]のチェックを外した場合，マネジメントモジュールが内蔵 LAN スイッチのデフォルトゲートウェイ設定を書き換えますので，お客様のネットワークに影響を与える可能性があります。変更の際は十分ご注意ください。

(3) IP アドレスの設定内容

各モジュールの管理インタフェースに接続するためには，次の項目を設定します。IPv6 ネットワークを使用する場合は，IPv4 アドレスの他に IPv6 アドレスを設定します。

項目		画面
IPv4 ネットワーク	IPv4 アドレス	各モジュールの管理インタフェースに IPv4 ネットワークで接続する場合の IPv4 アドレス，サブネットマスク，デフォルトゲートウェイを設定します。
	サブネットマスク	
	デフォルトゲートウェイ	
IPv6 ネットワーク	IPv6 アドレス	各モジュールの管理インタフェースに IPv6 ネットワークで接続する場合の IPv6 アドレス，プレフィックス，デフォルトゲートウェイを設定します。 IPv6 アドレスは RFC4291 で規定された形式で設定します。設定に際しては下記の URL を参考にしてください。 https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml
	プレフィックス	
	デフォルトゲートウェイ	

重要

- マネジメントモジュールに IPv6 ネットワークで接続する場合でも，IPv4 アドレスを削除することはできません。
- Web コンソールまたは，CLI コンソールでマネジメントモジュールに接続している IPv4 アドレスを変更した場合，IPv4 での接続が切断されます。
- Web コンソールまたは，CLI コンソールでマネジメントモジュールに接続している IPv6 アドレスを変更した場合，IPv6 での接続が切断されます。
- JP1/ServerConductor/Blade Server Manager，HA モニタ，HVM を使用する場合は，IPv4 ネットワークを使用してください。
- サーバブレードに IPv6 ネットワークで接続する場合は，サーバブレードファームウェアが IPv6 ネットワークをサポートしている必要があります。
- スイッチモジュールは IPv6 ネットワークでの接続に対応していません。
- マネジメントモジュールに IPv6 ネットワークで接続する場合，IPv6 アドレスにはグローバルユニキャストアドレスを設定してください。デフォルトゲートウェイを設定する場合は，マネジメントモジュールと同一リンクにあるルータのリンクローカルアドレスまたはグローバルユニキャストアドレスを設定してください。リンクローカルアドレスを設定することを推奨します。

(4) DNS サーバの設定

DNS サーバは，IPv4 アドレス用の DNS サーバと IPv6 アドレス用 DNS サーバをそれぞれ最大 3 台まで登録することができます。また，DNS サーバで名前解決する際に，IPv4 アドレス用の DNS サーバを優先するか，IPv6 アドレス用の DNS サーバを優先するか指定することができます。

設定した DNS サーバは，IPv4 用 DNS サーバおよび IPv6 用 DNS サーバをあわせて最大 3 つまで使われます。優先設定によって IPv4 用 DNS サーバあるいは IPv6 用 DNS サーバのどちらかを優先して使用し，3 つまで使用した時点で DNS サーバへのアクセスは終了します。

4 つ以上の DNS サーバ登録があった場合，優先度が 4 つ目以降の DNS サーバは使用されません。

例：

以下の設定の場合の使用順を示します。

- 設定

  優先度設定：IPv6

  IPv4 アドレス用の DNS サーバ 0：192.168.0.200

  IPv4 アドレス用の DNS サーバ 1：192.168.0.201

  IPv4 アドレス用の DNS サーバ 2：0.0.0.0 (設定なし)

  IPv6 アドレス用の DNS サーバ 0：2001:2000::100:100

  IPv6 アドレス用の DNS サーバ 1：2001:2000::100:101

  IPv6 アドレス用の DNS サーバ 2：0::0 (設定なし)

- 使用順

  (1). 2001:2000::100:100

  (2). 2001:2000::100:101

  (3). 192.168.0.200

  ※192.168.0.201 は 4 つ目となり，使用されません。

重要 DNS の設定を変更する場合，DNS の設定変更後に，以下の操作を実施してください。

- HTTP のサービスをいったん無効にしたあと，再度有効にしてください。
- SNMP の設定を再設定してください。

DNS サーバは，次の方法で設定します。

表 2-28 Web コンソールでの操作方法

項目	画面
IPv4 アドレス用 DNS サーバの表示，設定	Resources タブ → Systems → ネットワーク管理 → 管理 LAN → DNS タブ
IPv6 アドレス用 DNS サーバの表示，設定	
IPv4 アドレス/IPv6 アドレス優先度	

表 2-29 CLI コンソールでの操作方法

項目	コマンド
IPv4 アドレス用 DNS サーバの表示	show mgmt-module mgmt-lan
IPv4 アドレス用 DNS サーバの設定	set mgmt-module dns
IPv6 アドレス用 DNS サーバの表示	show mgmt-module mgmt-v6 setting
IPv6 アドレス用 DNS サーバの設定	set mgmt-module dns
IPv4 アドレス/IPv6 アドレス優先度の表示	show mgmt-module mgmt-v6 setting
IPv4 アドレス/IPv6 アドレス優先度の設定	set mgmt-module dns

2.3.7 マネジメントモジュール障害時のネットワーク構成

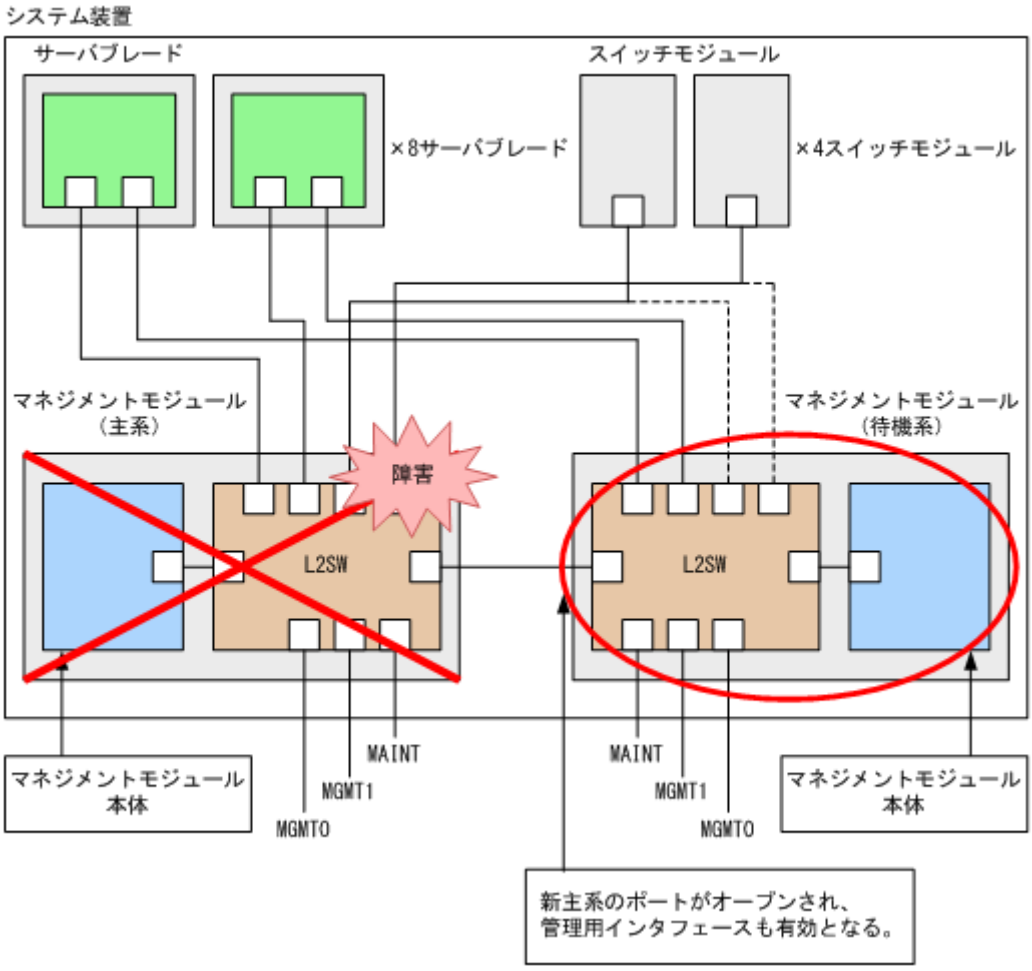
マネジメントモジュールが冗長化されている場合，主系マネジメントモジュールの管理用インタフェースのみが有効となり，待機系マネジメントモジュールのポートはクローズされています。

主系マネジメントモジュールに障害が発生した場合，待機系マネジメントモジュールが新しく主系となり動作を継続しますが，その時点で新しく主系となったマネジメントモジュールのポートはオープンされ，管理用インタフェースも有効となります。

新しく主系となったマネジメントモジュールの管理用インタフェースの IP アドレスは，主系だったマネジメントモジュールのものを引き継いで使用します。

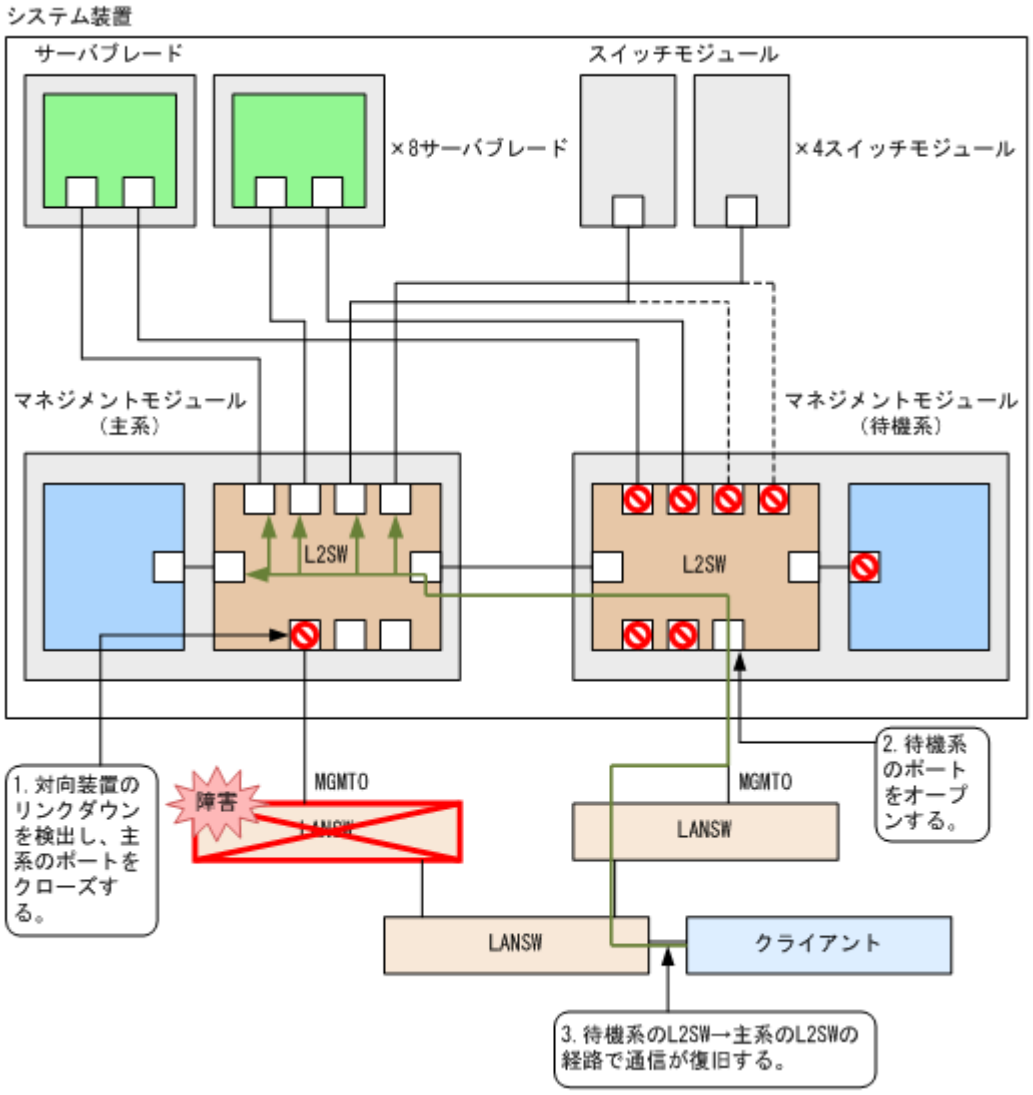
お客様がマネジメントモジュールの管理用インタフェースに接続する場合に，どちらのマネジメントモジュールが主系になっているかを意識する必要はありません。

参考 マネジメントモジュールが切り替わった際も管理用インタフェースと接続可能とするためには，LAN ケーブルが主系マネジメントモジュールと待機系マネジメントモジュールの両方に接続されている必要があります。



2.3.8 Link Fault Tolerance(LFT)

マネジメントモジュールを二重化している場合, 管理ネットワークの冗長化を組むことができます。本機能を Link Fault Tolerance(LFT)と呼びます。LFT の概要は次のとおりです。



LFT 対象となるポートは MGMT0 と MGMT1 です。これらは独立して有効無効を設定でき，工場出荷時はそれぞれ有効となっています。切り替えもそれぞれ独立して実施されるため，MGMT0 と MGMT1 を別のスイッチと接続している場合，片方の対向スイッチとの間で切り替え契機が発生すると，そのスイッチと接続されているポートのみが切り替えされます。

LFT 機能が有効の場合，主系マネジメントモジュールのポートが連続 3 秒間リンクダウンしたことを検出すると，当該ポートの切替を実施します。ポートの切替後，主系マネジメントモジュールのポートが連続 180 秒間リンクアップしたことを検出すると，当該ポートの復帰を実施します。

切替までの連続リンクダウン時間, および復帰までの連続リンクアップ時間は 1 秒～3600 秒の間で変更可能です。

表 2-30 Web コンソールでの操作方法

項目	画面
LFT 関連機能の表示，設定	Resources タブ → Systems → ネットワーク管理 → Link Fault Tolerance

2.4 セキュリティ

マネジメントモジュールと BMC の管理用インタフェースのセキュリティに関する機能について説明します。

2.4.1 マネジメントモジュールと BMC が提供する機能

マネジメントモジュールと BMC の管理用インタフェースが提供する機能を次に示します。

表 2-31 マネジメントモジュールが提供する機能

機能	サポートプロトコル	デフォルトポート番号	暗号化通信	サービス無効化	接続元 IP アドレス制限	ポート番号変更	備考
Web コンソール	HTTP	80	平文	○ ※1	○ ※14	○	※12
	HTTPS	443	暗号	○ ※1	○ ※14	○	※12 ※15
CLI コンソール	TELNET	23	平文	○ ※1	○ ※14	－	
	SSH	22	暗号	○ ※1	○ ※14	－	※2
ファイルの送受信	FTP	20，21	平文	○ ※1	○ ※14	－	
	SFTP	22	暗号	○ ※1	○ ※14	－	※13
E-mail 通報機能	SMTP	25(※11)	平文	○ ※3	－	○	
	SMTP(StartTLS)	465(※11)	暗号	○ ※3	－	○	
SNMP 機能(ポーリング機能)	SNMP(v1/v2c)	161	平文	○ ※4	○	○	
	SNMP(v3)	161	※5	○ ※4	○	○	
SNMP 機能(トラップ機能)	SNMP(v1/v2c)	162(※11)	平文	○ ※3	○	○	
	SNMP(v3)	162(※11)	※5	○ ※3	○	○	
LDAP 連携	LDAPS	636(※11)	暗号	○ ※3	－	○	
時刻同期	NTP	123(※11)	平文	○ ※3	－	－	
HCSM 連携(コマンド)	HTTPS	443	暗号	○ ※6	○	○	
HCSM 連携(アラート)	日立独自プロトコル	22611(※11)	暗号	○ ※3	○	○	
JP1/ServerConductor/Blade Server Manager 連携(コマンド)	日立独自プロトコル	21001	平文	○ ※7	○	○	
JP1/ServerConductor/Blade Server Manager 連携(アラート)	日立独自プロトコル	20079(※11)	平文	○ ※8	○	○	

機能	サポートプロトコル	デフォルトポート番号	暗号化通信	サービス無効化	接続元IPアドレス制限	ポート番号変更	備考
HA モニタ連携	日立独自プロトコル	※9	平文	○ ※10	－	○	
RADIUS 認証	RADIUS	1812	平文 ※16	○ ※3	－	○	

○：設定可能　－：設定不可

※1：全 IP アドレスからの接続を不許可にした状態となります。ポート自体は開いています。IPv4 ネットワークと IPv6 ネットワークの両方の接続が不可となります。

※2：バージョン 1 での接続はサポートしていません。

※3：機能自体を無効にすることで実現可能です。ポートに対する通信を行いません。

※4：機能自体を無効にすることで実現可能です。ポート自体は開いています。

※5：設定により，暗号化と平文を選択することができます。

※6：機能自体を無効にすることで実現可能です。また HTTPS を無効にした場合でも，無効化できます。ポート自体は開いています。

※7：管理サーバを登録しないことで実現可能です。ポート自体を閉塞します。

※8：管理サーバを登録しないことで実現可能です。ポートに対する通信を行いません。

※9：デフォルトではポート番号は未設定です。HA モニタを使用する際に，ユーザによって設定します。

※10：機能自体を無効にすることで実現可能です。ポート自体を閉塞します。

※11：マネジメントモジュールの通信先のポート番号です。

※12：Web コンソール接続を無効にする設定も可能です。

※13：SSH のサービス設定で一緒に設定します。

※14：IPv4 ネットワークと IPv6 ネットワークのそれぞれで設定が必要です。

※15：IPv6 アドレスで HTTPS アクセスを行った場合，常に証明書のエラー（警告）が表示されます。

※16：ユーザパスワードは暗号化され，RADIUS サーバに通知されます。

参考 【マネジメントモジュールファームウェア A0205 以降】
暗号化された通信をサポートした HVM では，マネジメントモジュールと HVM 間の通信が暗号化されます。

表 2-32 BMC が提供する機能

項目	サポートプロトコル	デフォルトポート番号	暗号化通信	サービス無効化	接続元IPアドレス制限	ポート番号変更
サーバブレード Web コンソール	HTTPS(※1)	443	暗号	○	○	－
IPMI over LAN	IPMI v1.5	623	平文	○	○	－
	IPMI v2.0	623	暗号	○	○	－
リモート	日立独自プロトコル	5001	暗号	○	○	○

項目	サポートプロトコル	デフォルトポート番号	暗号化通信	サービス無効化	接続元IPアドレス制限	ポート番号変更
コンソール						

○：設定可能　－：設定不可

※1：次に示すバージョンでは一部の通信に HTTP を用います。

- BS520H サーバブレード A1/B1 のサーバブレードファームウェア 05-02 以前
- BS520A サーバブレード A1 のサーバブレードファームウェア 02-57 以前
- BS540A サーバブレード A1/B1 のサーバブレードファームウェア 03-34 以前
- BS520H サーバブレード A2/B2 のサーバブレードファームウェアバージョン 04-21 以前

2.4.2 セキュリティ強度設定

マネジメントモジュールと BMC の管理用インタフェースにおいて，それぞれのセキュリティ強度を高める設定ができます。セキュリティ強度には"デフォルト"と"高"の設定があり，出荷時設定では"デフォルト"に設定されています。セキュリティ強度を"高"に設定すると，以下を行います。

- 暗号化通信が利用できる場合，平文での通信を不可とする
- 暗号化通信に対しては，セキュリティ強度の高い暗号化アルゴリズムのみ使用する

詳細は「2.4.3 セキュリティ強度と各機能との関係」を参照してください。

表 2-33 Web コンソールでの操作方法

項目	画面
マネジメントモジュールと BMC のセキュリティ強度設定の表示	Resources タブ → Systems → セキュリティ強度設定 → セキュリティ強度タブ
マネジメントモジュールと BMC のセキュリティ強度設定の設定	Resources タブ→ Systems → セキュリティ強度設定 → セキュリティ強度タブ → 編集

表 2-34 CLI コンソールでの操作方法

項目	コマンド
マネジメントモジュールと BMC のセキュリティ強度設定の表示	show security setting
マネジメントモジュールと BMC のセキュリティ強度設定の設定	set security strength

参考

- マネジメントモジュールのセキュリティ強度設定を高に設定した場合，TLS/SSL バージョン設定が TLS1.2 のみが有効設定となるので，TLS1.2 に対応した OS と Web ブラウザが必要です。HCSM を使用する際に必要な手順は，HCSM の取扱説明書，マニュアルを参照してください。
- HTTPS のサービスを無効に設定している場合に，マネジメントモジュールのセキュリティ強度設定を高に設定すると以下の機能が使用できなくなります。設定を変更する際は十分に注意願います。

  - Web コンソール

  - HCSM
- マネジメントモジュールのセキュリティ強度設定は，全サーバブレードが初期化完了状態で電源状態が OFF，かつ全マネジメントモジュールが初期化完了している状態で設定の変更が可能です。
- マネジメントモジュールのセキュリティ強度設定の変更を実施すると，全マネジメントモジュールが再起動します。再起動後の起動で設定変更が反映されます。

  BMC のセキュリティ強度設定の変更を実施した場合は，再起動は実施されず，即時反映されます。

- マネジメントモジュールのセキュリティ強度設定を高に設定した場合，マネジメントモジュールの Web コンソール接続には，Internet Explorer を使用してください。

  Firefox を用いてマネジメントモジュールの Web コンソールに接続する場合は，マネジメントモジュールのセキュリティ強度設定をデフォルトに設定してください。

- BMC のセキュリティ強度は，次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0175 以降

  サーバブレードファームウェア

  BS520H サーバブレード A1/B1 の場合，サーバブレードファームウェア 05-03 以降

  BS520A サーバブレード A1 の場合，サーバブレードファームウェア 02-58 以降

  BS540A サーバブレード A1/B1 の場合，サーバブレードファームウェア 03-35 以降

  BS520H サーバブレード A2/B2 の場合，サーバブレードファームウェア 04-22 以降

- BMC のセキュリティ強度の設定は, N+M コールドスタンバイで引き継ぐサーバブレードの設定情報には含まれません。N+M コールドスタンバイ構成を構築する場合は，現用サーバブレードと予備サーバブレードで BMC のセキュリティ強度の設定を同一にしてください。

- SNMP v1/v2c を使用してマネジメントモジュールに接続する管理ツールについては，マネジメントモジュールのセキュリティ強度の設定が"高"の場合は使用できません。

- HVM モードの場合，マネジメントモジュールと HVM が管理ネットワーク上で日立独自プロトコルを使用して制御通信を行っています。

  【マネジメントモジュールファームウェアバージョン A0205 以降】

  HVM が暗号化通信をサポートしている場合，マネジメントモジュールのセキュリティ強度設定にかかわらず，マネジメントモジュールと HVM 間の制御通信は暗号化されます。

2.4.3 セキュリティ強度と各機能との関係

セキュリティ強度の設定を変更した場合，マネジメントモジュールと BMC の各機能は設定により下記のプロトコル，暗号方式を使用します。

- マネジメントモジュール

機能	プロトコル	セキュリティ強度	
		"デフォルト"の場合の挙動	"高"の場合の挙動
Web コンソール	HTTP	使用可能	使用不可(※1)
	HTTPS	使用可能(※6)	使用可能(TLS 1.2)(※2)
CLI コンソール	TELNET	使用可能	使用不可(※1)
	SSH	使用可能(SSHv2)	使用可能(SSHv2)
ファイルの送受信	FTP	使用可能	使用不可(※1)
	SFTP	使用可能(SSHv2)	使用可能(SSHv2)
SNMP 機能	SNMP(v1/v2c)	使用可能	使用不可(※3)
	SNMP(v3)	使用可能	使用可能
Email 通報機能	SMTP	使用可能	使用不可(※4)
	SMTP(StartTLS)	使用可能(※6)	使用可能(TLS 1.2)
LDAP 連携	LDAPS	使用可能(※6)	使用可能(TLS 1.2)
時刻同期	NTP	使用可能	使用可能
HCSM 連携	HTTPS および日立独自プロトコル	使用可能(※6)	使用可能(TLS 1.2)

機能	プロトコル	セキュリティ強度	
		"デフォルト"の場合の挙動	"高"の場合の挙動
JP1/ServerConductor/Blade Server Manager 連携	日立独自プロトコル	使用可能(※5)	使用可能(※5)
HA モニタ連携	日立独自プロトコル	使用可能(※5)	使用可能(※5)

※1：ポートを閉塞します。

※2：使用する SSL/TLS バージョンに対応したブラウザが必要です。

※3：マネージャからの要求に対して無応答となります。トラップを発行しません。

※4：E-mail を発行しません。

※5：ユーザ設定により通信不可とすることが可能です。

※6：使用できる暗号化のプロトコルは，SSL3.0，および TLS1.0/1.1/1.2 です。通信プロトコルが HTTPS の場合は，使用する SSL/TLS バージョンに対応したブラウザが必要です。

なお，出荷時の設定では，SSL3.0 は"無効"に設定されています。SSL3.0 プロトコルには，通信の一部が解読されてしまう脆弱性が存在します。そのため，SSL3.0 を利用する必要がない場合は，SSL3.0 の設定は"無効"のままで運用することを推奨します。設定については，「2.4.5 TLS/SSL バージョン設定機能」を参照してください。

参考 セキュリティ強度を"高"に設定した場合，あるいはセキュリティ強度を"通常"に設定した状態で TLS1.2 以外での通信を不可と設定した場合，TLS1.2 に非対応の HCSM とは接続できません。HCSM を使用する際に必要な手順は，HCSM の取扱説明書，マニュアルを参照してください。

- BMC

機能	プロトコル	セキュリティ強度	
		"デフォルト"の場合の挙動	"高"の場合の挙動
サーバブレード Web コンソール	HTTP	使用不可(※1)	使用不可(※1)
	HTTPS	使用可能 (SSL3.0，TLS1.0/1.1/1.2) (※4)	使用可能(TLS 1.2)
IPMI over LAN	IPMI v1.5	使用可能	使用不可(※2)
	IPMI v2.0	使用可能	使用可能(※3)
リモートコンソール	日立独自プロトコル	使用可能 (SSL3.0，TLS1.0/1.1/1.2) (※4)	使用可能(TLS 1.2)

※1：次に示すバージョンではポートを閉塞します。

- BS520H サーバブレード A1/B1 のサーバブレードファームウェア 05-03 以降
- BS520A サーバブレード A1 のサーバブレードファームウェア 02-58 以降
- BS540A サーバブレード A1/B1 のサーバブレードファームウェア 03-35 以降
- BS520H サーバブレード A2/B2 のサーバブレードファームウェアバージョン 04-22 以降

※2：IPMI v1.5 LAN Session Startup 時に接続拒否します。

※3：CipherSuite ID が 3 のときかつ Username/Password がいずれも空でないときのみ接続可能です。

※4：BS520X サーバブレード B1/B2，BS520H サーバブレード B3 では，SSL3.0 は非サポートのため，使用できません。

2.4.4 セキュリティ強度の設定による機能比較

セキュリティ強度の設定による機能の違いを比較します。

・ SSL/TLS

暗号スイート	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
TLS_RSA_WITH_AES_128_CBC_SHA	○	×	○	○
TLS_RSA_WITH_AES_256_CBC_SHA	○	×	○	○
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	○	×	×	×
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	○	×	×	×
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	○	○	×	×
TLS_RSA_WITH_AES_128_CBC_SHA256	○	○	○	○
TLS_RSA_WITH_AES_256_CBC_SHA256	○	○	○	○
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	○	○	×	×
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	○	×	×	×
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	○	○	×	×
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	○	×	×	×
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	○	○	×	×
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	○	×	×	×
TLS_DHE_RSA_WITH_AES_256_SHA	○	×	×	×
TLS_DHE_DSS_WITH_AES_256_SHA	○	×	×	×
TLS_RSA_WITH_AES_256_GCM_SHA384	○	○	×	×
TLS_RSA_WITH_AES_128_GCM_SHA256	○	○	×	×
TLS_EDH_RSA_WITH_3DES_EDE_CBC_SHA	○	×	×	×
TLS_EDH_DSS_WITH_3DES_EDE_CBC_SHA	○	×	×	×
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	○	○	×	×
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	○	×	×	×
TLS_RSA_WITH_3DES_EDE_CBC_SHA	○	×	○	×
TLS_RSA_WITH_RC4_128_MD5	○	×	×	×
TLS_RSA_WITH_RC4_128_SHA	○	×	○	×

サーバ証明書(公開鍵アルゴリズム)	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
RSA1024	×	×	×	×
RSA2048	○	○	○	○
RSA4096	×	×	×	×

サーバ証明書(公開鍵アルゴリズム)	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
DSA1024	×	×	×	×

サーバ証明書(署名アルゴリズム)	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
SHA1 検証	○	○	×	×
SHA1 作成	○	×	×	×
SHA256 検証	○	○	×	×
SHA256 作成	×	○	×	×
SHA384 検証	×	×	○	○
SHA384 作成	×	×	○	○

・ SSH

ホスト鍵アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
RSA1024	×	×	×	×
RSA2048	○	○	○	○
RSA4096	×	×	×	×
DSA1024	○	×	○	×

鍵交換アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
diffie-hellman-group1-sha1	○	○	○	○
diffie-hellman-group14-sha1	○	○	○	○
diffie-hellman-group-exchange-sha1	○	○	○	○
diffie-hellman-group-exchange-sha256	○	○	○	○

暗号アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
3des	×	×	×	×
3des-cbc	○	○	○	○
aes128-cbc	○	○	○	○
aes192-cbc	○	○	○	○
aes256-cbc	○	○	○	○
aes128-ctr	○	○	○	○
aes192-ctr	○	○	○	○
aes256-ctr	○	○	○	○
blowfish-cbc	○	×	○	×
cast128-cbc	○	×	○	×
arcfour	○	×	○	×

暗号アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
arcfour128	○	×	○	×
arcfour256	○	×	○	×
rijndael-cbc@lysator.liu.se	○	×	○	×

メッセージ認証アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
hmac-md5	×	×	○	×
hmac-sha1	○	○	○	○
hmac-ripemd160	×	×	○	×
hmac-ripemd160@openssh.com	×	×	○	×
umac-64@openssh.com	○	×	○	×
hmac-sha1-96	○	○	○	○
hmac-md5-96	○	○	○	×
hmac-sha2-256	○	○	○	○
hmac-sha2-512	○	○	○	○

- SNMP v3

暗号アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
なし	○	×	SNMP 非サポート	
DES	○	×		
AES128	○	○		

認証アルゴリズム	マネジメントモジュール		サーバブレード	
	セキュリティ強度		セキュリティ強度	
	デフォルト	高	デフォルト	高
なし	○	×	SNMP 非サポート	
MD5	○	×		
SHA1	○	○		

2.4.5 TLS/SSL バージョン設定機能

マネジメントモジュールと BMC の管理用インタフェースにおいて，それぞれの暗号通信時に使用する TLS/SSL バージョンに有効/無効設定ができます。各 TLS/SSL のバージョンごとに設定でき，出荷時設定は以下のように設定されています。

- マネジメントモジュール

TLS/SSL バージョン	出荷時設定
SSL3.0	無効(※1)
TLS1.0	有効

TLS/SSL バージョン	出荷時設定
TLS1.1	有効
TLS1.2	有効

※1：SSL3.0 プロトコルには，通信の一部が解読されてしまう脆弱性が存在します。そのため，SSL3.0 を利用する必要がない場合は，SSL3.0 の設定は"無効"のままで運用することを推奨します。

- BMC

TLS/SSL バージョン	出荷時設定
SSL3.0	有効(※1)
TLS1.0	有効
TLS1.1	有効
TLS1.2	有効

※1：BS520X サーバブレード B1/B2，BS520H サーバブレード B3 では，SSL3.0 は非サポートのため，SSL3.0 の設定項目はありません。

表 2-35 Web コンソールでの操作方法

項目	画面
マネジメントモジュールの TLS/SSL バージョン設定の表示	Resources タブ → Systems → セキュリティ強度設定 → TLS/SSL バージョンタブ
マネジメントモジュールの TLS/SSL バージョン設定の設定	Resources タブ → Systems → セキュリティ強度設定 → TLS/SSL バージョンタブ→編集
BMC の TLS/SSL バージョン設定の表示	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → BMC タブ
BMC の TLS/SSL バージョン設定の設定	Resources タブ → Modules → 全モジュール → サーバブレード →サーバブレード x → BMC タブ → 編集

表 2-36 CLI コンソールでの操作方法

項目	コマンド
マネジメントモジュールの TLS/SSL バージョン設定の表示	show security setting
マネジメントモジュールの TLS/SSL バージョン設定の設定	set security tls mgmt-module

重要 全 TLS/SSL バージョン設定を無効に設定することはできません。

参考

- マネジメントモジュールのセキュリティ強度設定を"高"に変更した場合，マネジメントモジュールの TLS バージョン設定は TLS1.2 のみ有効が設定され，SSL3.0，TLS1.0/1.1 は，無効が設定されます。変更はできません。
- セキュリティ強度を"高"に設定した場合，あるいはセキュリティ強度を"通常"に設定した状態で TLS1.2 以外での通信を不可と設定した場合，TLS1.2 に非対応の HCSM とは接続できません。HCSM を使用する際に必要な手順は，HCSM の取扱説明書，マニュアルを参照してください。
- BMC の TLS/SSL バージョン設定は Web コンソールのみから実施可能です。
- サーバブレードのセキュリティ強度設定を"高"に変更した場合，サーバブレード Web コンソールおよびリモートコンソールの TLS バージョン設定は TLS1.2 のみ有効が設定され，SSL3.0，TLS1.0/1.1 は，無効が設定されます。変更はできません。SMASH(WS-Management)は TLS1.0 を使用します。
- BS520H サーバブレード A1/B1，BS520A サーバブレード A1，BS540A サーバブレード A1/B1 では，BMC の TLS/SSL バージョン設定はサポートしていません。

- BMC の TLS/SSL バージョン設定は，次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0175 以降

  サーバブレードファームウェア

  BS520H サーバブレード A1/B1 の場合，サーバブレードファームウェア 05-03 以降

  BS520A サーバブレード A1 の場合，サーバブレードファームウェア 02-58 以降

  BS540A サーバブレード A1/B1 の場合，サーバブレードファームウェア 03-35 以降

  BS520H サーバブレード A2/B2 の場合，サーバブレードファームウェア 04-22 以降

- BMC の TLS/SSL バージョン設定は，N+M コールドスタンバイで引き継ぐサーバブレードの設定情報には含まれません。N+M コールドスタンバイ構成を構築する場合は，現用サーバブレードと予備サーバブレードで BMC のセキュリティ強度の設定を同一にしてください。

2.4.6 マネジメントモジュールが提供するサービスの IP アドレス制限設定

FTP，TELNET，SSH，HTTP，HTTPS の各サービスは，サービス単位で次の設定を行うことができます。

- サービス自体の有効，無効設定
- 接続可能 IP アドレスの設定（IPv4 アドレスと IPv6 アドレスのそれぞれで設定）
- ポート番号変更(HTTP，HTTPS のみ設定変更可能)

接続可能 IP アドレスの設定は, IPv4 ネットワークと IPv6 ネットワークのそれぞれで設定が必要です。接続可能 IP アドレスの設定をした場合，設定した IP アドレス以外からの接続を拒絶します。接続可能 IP アドレスはネットワークアドレスによる範囲指定が可能で，IPv4 ネットワークと IPv6 ネットワークのそれぞれのサービスごとに一つ設定することができます。サービス自体を無効とした場合，そのサービスを使用することができなくなります。

重要

- SSH の接続設定を無効にして接続した場合，もしくは SSH の接続可能 IP アドレスを設定し，設定した IP アドレス以外から接続した場合，お使いのターミナルソフトによってはログイン画面まで表示されることがあります。その場合，認証で必ず失敗し，ログインはできません。
- 接続可能 IP アドレスのネットワークアドレスのサブネットマスクは, 255.255.255.255 以外を設定してください。

表 2-37 Web コンソールでの操作方法

項目	画面
TELNET の接続設定の表示，設定	Administration タブ → サービス → Telnet タブ
FTP の接続設定の表示，設定	Administration タブ → サービス → FTP タブ
SSH の接続設定の表示，設定	Administration タブ → サービス → SSH/SFTP タブ
HTTP の接続設定の表示，設定	Administration タブ → サービス → HTTP タブ
HTTPS の接続設定の表示，設定	Administration タブ → サービス → HTTPS タブ

表 2-38 CLI コンソールでの操作方法

項目	コマンド
TELNET の接続設定の表示	show remote-access protocol telnet
TELNET の接続設定の設定	set remote-access protocol telnet
FTP の接続設定の表示	show remote-access protocol ftp
FTP の接続設定の設定	set remote-access protocol ftp

項目	コマンド
SSH の接続設定の表示	show remote-access protocol ssh
SSH の接続設定の設定	set remote-access protocol ssh
HTTP の接続設定の表示	show remote-access protocol http
HTTP の接続設定の設定	set remote-access protocol http
HTTPS の接続設定の表示	show remote-access protocol https
HTTPS の接続設定の設定	set remote-access protocol https

表 2-39 LCD タッチコンソールでの操作方法

項目	画面
接続設定の表示，設定	システム構築 → サービス設定

2.4.7 認証情報暗号化設定

マネジメントモジュールでは，ユーザ ID，パスワードおよび秘密鍵などの認証情報を暗号化することができます。出荷時設定では"無効"に設定されています。認証情報の暗号化設定を"有効"にすることでマネジメントモジュールにおける認証情報を暗号化します。

認証情報を暗号化することで，マネジメントモジュールがシステム装置外に持ち出され，記憶媒体を読み取られた際に，認証情報が外部に漏れることを防止することができます。

表 2-40 CLI コンソールでの操作方法

項目	コマンド
認証情報の暗号化設定の表示	`show user authentication encryption`
認証情報の暗号化設定の設定	`set user authentication encryption`

重要

- 認証情報の暗号化設定を変更する場合，操作中に認証情報を含めた構成情報の設定を変更しないでください。操作中に構成情報の設定を変更しても，設定は反映されません。
- 認証情報を含めた構成情報の更新中に，認証情報の暗号化設定を変更しないでください。構成情報の更新中に暗号化設定を変更しようとすると操作に失敗します。
- 認証情報の暗号化設定を変更した場合，マネジメントモジュールは再起動します。暗号化設定は，再起動後から反映されます。
- 認証情報の暗号化設定を変更して再起動した後，設定が変更されたか確認してください。設定が変更されていない場合は，再度，設定変更をしてください。
- 認証情報の暗号化設定を"無効"に設定した場合，認証情報は初期設定に戻ります。工場出荷時のデフォルトで登録されているアカウントでログインして，認証情報を再設定してください。
- 認証情報暗号化設定を"有効"に設定した後，A0245 より前のマネジメントモジュールファームウェアにアップデートを実施する場合，必ず，認証情報の暗号化設定を"無効"に変更してからアップデートを実施してください。

参考

- 認証情報の暗号化設定を"有効"に変更する場合，変更前に構成情報をバックアップすることを推奨します。構成情報をバックアップしておくと，問題発生時に，暗号化設定前の認証情報に戻すことができます。

2.5 システム装置設定

システム装置のシャーシ ID と言語設定について説明します。

2.5.1 シャーシ ID 設定

システム装置には，シャーシ ID と呼ぶ識別子を登録することができます。シャーシ ID は 20 文字の文字列を設定することができ，工場出荷時はサーバシャーシ製造番号の一部が設定されています。シャーシ ID は，次で表示され，装置識別に使用できます。

- Web コンソール，CLI コンソール，LCD タッチコンソールでの接続装置の表示。
- JP1/ServerConductor/Blade Server Manager での装置表示。

表 2-41 Web コンソールでの操作方法

項目	画面
シャーシ ID の表示，設定	Resources タブ → Modules → 全モジュール → シャーシ → 設定タブ → シャーシ ID 設定

表 2-42 CLI コンソールでの操作方法

項目	コマンド
シャーシ ID の表示	show chassis setting
シャーシ ID の設定	set chassis id

重要 複数のサーバシャーシでシャーシ ID の値を重複させないでください。

2.5.2 言語設定

本装置は，日本語，English の表示をサポートしています。システム装置に対して，日本語/English の言語切替が可能です。

ただし，アカウント設定で言語の項目が「日本語」もしくは「English」となっているアカウントで Web コンソールや CLI コンソールにログインした場合，システム装置の設定には従わず，アカウント設定で設定された言語で表示されます。

表 2-43 Web コンソールでの操作方法

項目	画面
言語設定の表示と設定	Administration タブ → 言語設定

表 2-44 CLI コンソールでの操作方法

項目	コマンド
言語設定の表示	show language system
言語設定の設定	set language system

参考 言語設定が日本語であっても，英語で表示される項目があります。

2.6 電源制御

システム装置の電源制御について説明します。

2.6.1 システム装置の電源を入れる

システム装置は AC 電源を投入すると自動的に起動します。

設定により，システム装置の起動と同期してサーバブレードを起動することができます。

詳細は「2.6.5 電源復旧時のサーバブレード動作設定」を参照してください。

2.6.2 システム装置の電源を切る

システム装置の電源を切る場合は，マネジメントモジュールから操作します。すべてのサーバブレードの電源を切った後に実施してください。

表 2-45 Web コンソールでの操作方法

項目	画面
システム装置のシャットダウン	Resources タブ → Modules → 全モジュール → シャーシ → Action → シャットダウン

表 2-46 CLI コンソールでの操作方法

項目	コマンド
システム装置のシャットダウン	shutdown chassis

表 2-47 LCD タッチコンソールでの操作方法

項目	画面
システム装置のシャットダウン	ハードウェア保守 → サーバシャーシ(SC) → シャーシシャットダウン

2.6.3 サーバブレードの電源を操作する

マネジメントモジュールから，サーバブレードの電源に関する次の操作を実施することができます。

サーバブレードの電源操作

- 電源 ON
- 電源 OFF
- 強制電源 OFF
- リセット
- NMI 発行
- BMC リスタート

重要

- 電源 OFF は，OS の種類および OS の状態によっては実行されない場合があります。
  サーバブレードの電源 OFF は，OS 上の操作や JP1/ServerConductor にて実施することを推奨します。
- BMC リスタートは，サーバブレードの障害発生時のリカバリ手段です。
  通常運用では実施しないでください。

参考 電源 OFF は，サーバブレードの電源ボタンの 1 秒押しのエミュレーションです。
強制電源 OFF は，サーバブレードの電源ボタンの 4 秒押しのエミュレーションです。

表 2-48 Web コンソールでの操作方法

項目	画面
サーバブレードの電源 ON，電源 OFF，強制電源 OFF， ハードリセット，NMI 発行	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 状態タブ
BMC の再起動	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → BMC タブ

表 2-49 CLI コンソールでの操作方法

項目	コマンド
サーバブレードの電源 ON	poweron blade
サーバブレードの電源 OFF，強制電源 OFF	poweroff blade
サーバブレードのハードリセット，NMI 発行	reset blade
BMC の再起動	bmc-reset blade

2.6.4 スイッチモジュールの電源を操作する

マネジメントモジュールから，スイッチモジュールの電源 ON と電源 OFF を実施することができます。

参考 システム装置の AC 電源投入時は，スイッチモジュールの電源は自動的に起動します。
電源 ON の操作は不要です。

表 2-50 Web コンソールでの操作方法

項目	画面
スイッチモジュールの電源操作	Resources タブ → Modules → 全モジュール → スイッチモジュール → スイッチモジュール x

2.6.5 電源復旧時のサーバブレード動作設定

マネジメントモジュールの設定により，システム装置の電源の投入時のサーバブレードの動作を次のいずれかから選択することができます。

- 電源 OFF
- 電源 ON
- 障害発生前の状態(前回の AC 切断時の電源状態が ON なら ON する)

これにより，停電後の電源復旧時などに，サーバブレードの電源も自動的に復電させることが可能です。

また，電源 ON する場合，システム装置が起動してからサーバブレードの電源を ON するまでの待ち時間を 0 分から 60 分の間で設定することができます。これにより，サーバブレード起動前に他の周辺機器を起動しておく必要がある場合に，周辺機器の電源の ON が完了するのを待ってからサーバブレードの電源 ON をさせることができます。

重要

- N+M コールドスタンバイの予備系となるサーバブレードでは，本設定は「電源 OFF」としてください。予備系が「電源 ON」に設定されていると，そのサーバブレードへの N+M 切替が実施できません。
- N+M コールドスタンバイ支援機能が有効のサーバブレードでは，UEFI セットアップメニューで電源復旧時のサーバ自動電源投入が正しく動作しないことがあります。必ず本設定で復電設定を実施してください。

参考 SMP 構成のサーバブレードは，プライマリサーバブレードに指定された環境設定値で動作します。ノンプライマリサーバブレードに対し，プライマリサーバブレードと異なる環境設定値を設定しないようにしてください。

表 2-51 Web コンソールでの操作方法

項目	画面
電源復旧時のサーバブレード動作設定	Resources タブ → Modules → サーバブレード → サーバブレード x → 設定タブ

2.7 サーバブレードの遠隔操作

リモートコンソールまたは OS コンソールを使用した，サーバブレードの遠隔操作について説明します。

2.7.1 リモートコンソールによる操作

本装置では，各サーバブレードのグラフィカルコンソールとしてリモートコンソールを使用します。

リモートコンソールによって，VGA 表示，キーボード，マウス操作，リモート CD/DVD，リモート FD などを遠隔地から実行することができます。

リモートコンソールの操作方法の詳細は，「*BladeSymphony BS500 リモートコンソール ユーザーズガイド*」を参照してください。

リモートコンソールは，Web コンソール，もしくはシステムコンソールの Web ブラウザから起動することができます。また，マネジメントモジュールのコンソールから，リモートコンソールのセッション管理に関する操作が実施可能です。

BMC のリモートコンソールのセッション状態の表示と，セッションの強制切断が可能です。

表 2-52 CLI コンソールでの操作方法

項目	コマンド
リモートコンソールのセッション情報表示	show blade bmc session
リモートコンソールのセッション切断	disconnect blade bmc session

重要 SMP 構成の場合，リモートコンソールの接続先となるサーバブレードにはプライマリサーバブレードを選択してください。

2.7.2 OS コンソールによる操作

OS コンソールは，サーバブレードのシリアルポート入出力をシステムコンソールに LAN 経由で転送し，シリアルコンソールの遠隔操作を行う機能です。

重要 OS コンソールでは次の操作は実施できません。これらの操作をする場合は，グラフィカルなコンソールであるリモートコンソールを使用してください。

- OS 起動前の操作
- OS のインストール操作

2.7.3 OS コンソール使用前の準備

OS コンソールを使用する場合は，次の事前準備を行ってください。

(1) ターミナルソフトウェアのインストール

システムコンソールには，事前にターミナルソフトウェアをインストールしておきます。(Linux などの OS では，OS の初期状態で既にインストールされている場合があります)

ターミナルソフトウェアには，次の機能が必要です。

- TELNET を利用できること（TELNET 接続を行う場合）
- SSH version2 を利用できること（SSH 接続を行う場合）

重要

- 入力／出力文字は，ターミナルソフトウェアの仕様により制限される場合があります。また，エミュレーションするターミナルの種類は利用する OS のターミナルと同一に設定してください。
- ターミナル設定により，日本語の出力ができない場合があります。

(2) OS シリアルポート設定の確認

OS コンソールは，サーバブレードの COM2 ポートを利用しています。

サーバブレードの OS の種類により設定方法が異なります。

次を参照し，設定を確認してください。

Windows の場合

OS の COM2 のポート設定が，次のようになっていることを確認してください。

表 2-53 COM2 のポート設定

項目	内容
ポート	COM2
ボーレート	115200
データ	8bit
パリティ	none
ストップ	1bit
フロー制御	none
推奨端末タイプ	VT100

重要 Windows Special Administration Console (SAC)に，OS コンソールを使用することはできません。

Red Hat Enterprise Linux の場合

OS のパラメータを，次のように設定してください。

表 2-54 パラメータ設定例

項目	内容	備考
/boot/grub/grub.conf の設定	各 kernel 行の末尾に console=tty0 console=ttyS1,115200 を追加	－
/etc/inittab の設定	最終行に co:2345:respawn:/sbin/agetty 115200 ttyS1 vt100 を追加 変更後，init q を実行	Linux 6.2 以降では不要
/etc/sysconfig/kudzu の設定	SAFE=yes に変更（無い場合には追加）	Linux 6.2 以降では不要

項目	内容	備考
/etc/security の設定	ttyS1 を追加	−

参考

- Linux の Login モードは，"Text mode"でインストールする必要があります。
- "Graphic mode"でインストールした場合，"Text mode"への変更が必要です。
  変更方法は，OS のマニュアルなどを参照してください。

2.7.4 OS コンソールの使用方法

OS コンソールは，マネジメントモジュールの CLI コンソールから起動できます。

重要 SMP 構成の場合，OS コンソールの接続先となるサーバブレードにはプライマリサーバブレードを選択してください。

表 2-55 CLI コンソールでの操作方法

項目	コマンド
OS コンソールの起動	change console -b

参考

- BS520H サーバブレード A1/B1/A2/B2/B3，BS520A サーバブレード A1，BS540A サーバブレード A1/B1 の場合，他の端末で OS コンソールを使用している場合は，OS コンソールを起動することはできません。
- BS520X サーバブレード B1/B2 の場合，複数の端末で 16 個まで OS コンソールを同時に使用できます。
- OS コンソールを使用中にネットワークが切断された場合，OS コンソールのセッションがしばらく残り続けることがあります。その場合，『リモートコンソールのセッション切断』を行うことで，この状態を解除することができます。
  詳細は「2.7.1 リモートコンソールによる操作」を参照してください。

2.7.5 OS コンソールの使用時の注意事項

OS コンソールを使用する場合は，次の注意事項を守ってください。

(1) OS コンソールの操作について

- 入力操作
  キーボードからの入力を前提としており，ファイル転送などによる高速なデータ入力には対応しておりません。キーボードから入力操作を行ってください。
- セッション切断時の回復方法
  ご利用の環境によっては，画面表示が著しく遅くなったり，ターミナルソフトウェアのセッションが切断されたりすることがあります。このような場合は，再度 OS コンソールに接続しなおしてください。また，文字出力が多いアプリケーションでは，出力処理による性能低下を招く場合があります。これらの用途では，事前に評価を実施し，必要に応じて表示出力を抑止してください。
- 文字の転送漏れ
  OS コンソールへの文字入力を，カットアンドペースト操作で行う場合，文字の転送漏れが発生することがあります。

(2) 文字コード，表示色について

システムコンソールとサーバブレードとの間で，文字コード，表示色の扱いが異なる場合があります。次のような［現象］が起きた場合には，［対処方法］を試してください。

表 2-56 現象と対処方法

項目	内容
現象	システムコンソールの表示が，文字化けする。
原因	通信条件の設定が間違っている。 システムコンソール側のソフトウェアで不適切な文字セットが選択されている。 送出側のソフトウェア（Windows/Linux など）で，不適切な文字コードを送出している。
対処方法	「2.7.3 OS コンソール使用前の準備」を参照し，システムコンソール側のソフトウェアの設定が同じであるか確認してください。 システムコンソール側のソフトウェアで，適切な文字セットを選択し直してください。 送出側ソフトウェアのマニュアルなどを参照してください。

(3) Red Hat Enterprise Linux システム要求キー機能について

OS コンソールにおいてシステム要求キー機能を使用するには，次のシーケンスを送信してください。

表 2-57 シーケンスの送信内容

項目	内容
TELNET 接続の場合	TELNET 仕様による IAC(Interpreted AsCommand) break シーケンス，または[Ctrl]+[¥]を送ってください。ターミナルソフトウェアからの break 信号の送信方法は，ソフトウェアごとに異なります。 詳細は，各ターミナルソフトウェアのマニュアルを参照してください。
SSH 接続の場合	[Ctrl]+[¥]を送ってください。

2.8 識別 LED(LID)の操作

次のモジュールには識別 LED(LID)が搭載されており，マネジメントモジュールのコンソールから点灯，消灯を実施することができます。LID を使用することで，システム装置を直接操作する作業者に，どのモジュールをリモートで使用中かなどの情報を間接的に通知することができます。

- フロントパネル
- マネジメントモジュール
- サーバブレード
- スイッチモジュール

参考 SMP 構成のサーバブレードも，それぞれのサーバブレードの LID を使用できます。

表 2-58 Web コンソールでの操作方法

項目	画面
フロントパネルの LID の表示，操作	Resources タブ → Modules → 全モジュール → シャーシ → フロントパネルタブ
マネジメントモジュールの LID の表示，操作	Resources タブ → Modules → 全モジュール → マネジメントモジュール → マネジメントモジュール x

項目	画面
サーバブレードの LID の表示，操作	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x
スイッチモジュールの LID の表示，操作	Resources タブ → Modules → 全モジュール → スイッチモジュール → スイッチモジュール x

表 2-59 CLI コンソールでの操作方法

項目	コマンド
フロントパネルの LID の表示	show front-panel status
フロントパネルの LID の操作	set front-panel led
マネジメントモジュールの LID の表示	show mgmt-module status
マネジメントモジュールの LID の操作	set mgmt-module led
サーバブレードの LID の表示	show blade status
サーバブレードの LID の操作	set blade led
スイッチモジュールの LID の表示	show sw-module status
スイッチモジュールの LID の操作	set sw-module led

表 2-60 LCD タッチコンソールでの操作方法

項目	画面
フロントパネルの LID の表示，操作	ハードウェア保守 → サーバシャーシ(SC) → LID ON/OFF
マネジメントモジュールの LID の表示，操作	ハードウェア保守 → マネジメントモジュール(MM) → LID ON/OFF
サーバブレードの LID の表示，操作	ハードウェア保守 → サーバブレード(SB) → LID ON/OFF
スイッチモジュールの LID の表示，操作	ハードウェア保守 → スイッチモジュール(SW) → LID ON/OFF

2.9 装置内の各モジュールの設定

システム装置内の各モジュールの設定について説明します。

2.9.1 マネジメントモジュールから実施可能な各モジュールの設定

システム装置には，マネジメントモジュールの他に，サーバブレード，スイッチモジュールなどのモジュールが搭載されており，システム構築，運用のためにはこれらのモジュールの設定をする必要があります。

本装置では，マネジメントモジュールのコンソールから，これらのモジュールの設定をする，もしくはこれらのモジュールのコンソールにリンクで飛ぶことが可能です。このため，マネジメントモジュールのコンソールに接続すれば，他のコンソールに接続することなく，シームレスにシステム装置内の各モジュールの設定を行うことができます。

次に，マネジメントモジュールのコンソールから実施可能な各モジュールの設定項目を示します。

表 2-61 Web コンソールから実施可能な各モジュールの設定項目

対象	マネジメントモジュールのコンソールから設定	当該モジュールのコンソールへのリンク	備考
サーバブレード(BMC)設定	○	－	－
サーバブレード(UEFI)設定	○ (一部)	－	－
HVM 設定	○ (一部)	－	詳細は「2.18 HVM 連携」を参照してください。
Hitachi 1Gb LAN スイッチモジュール(20 ポート)設定	○ (一部)	－	－
Hitachi 1Gb LAN スイッチモジュール(40 ポート)設定	○ (一部)	－	－
Hitachi 1/10Gb LAN スイッチモジュール設定	○ (一部)	－	－
Brocade 10Gb DCB スイッチモジュール	－	－	－
Brocade 8Gb ファイバチャネルスイッチモジュール設定	－	○	－
Brocade 8/16Gb ファイバチャネルスイッチモジュール設定	－	○ (※1)	－
Brocade 16Gb ファイバチャネルスイッチモジュール設定	－	○ (※1)	－
Hitachi ファイバチャネル拡張カード設定	○	－	－

○：設定可能　－：設定不可

※1：スイッチモジュールのアカウント入力なしで，スイッチモジュールの Web コンソールにログインすることができます。(シングルサインオン)

表 2-62 CLI コンソールから実施可能な各モジュールの設定項目

対象	マネジメントモジュールのコンソールから設定	当該モジュールのコンソールへのリンク	備考
サーバブレード(BMC)設定	－	－	－
サーバブレード(UEFI)設定	－	－	－
HVM 設定	－	○ (※1)	－
Hitachi 1Gb LAN スイッチモジュール(20 ポート)設定	－	○ (※2)	－
Hitachi 1Gb LAN スイッチモジュール(40 ポート)設定	－	○ (※2)	－
Hitachi 1/10Gb LAN スイッチモジュール設定	－	○ (※2)	－
Brocade 10Gb DCB スイッチモジュール	－	○ (※2)	－
Brocade 8Gb ファイバチャネルスイッチモジュール設定	－	○	－
Brocade 8/16Gb ファイバチャネルスイッチモジュール設定	－	○ (※2)	－
Brocade 16Gb ファイバチャネルスイッチモジュール設定	－	○ (※2)	－
Hitachi ファイバチャネル拡張カード設定	－	－	－

○：設定可能　－：設定不可

※1：HVM 起動中に OS コンソールに接続することで，HVM コンソールに接続することができます。HVM コンソールの詳細は「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

※2：スイッチモジュールのアカウント入力なしで，スイッチモジュールのコンソールにログインすることができます(シングルサインオン)。

参考 各モジュールの設定をするためには，アカウントに適切なロールを設定する必要があります。
詳細は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」，「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

表 2-63 Web コンソールでの操作方法

項目	画面
サーバブレード(BMC)設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → BMC タブ
サーバブレード(UEFI)設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → EFI タブ
HVM 設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → LPAR タブ
Hitachi LAN スイッチモジュール設定	Resources タブ → Modules → 全モジュール → スイッチモジュール → スイッチモジュール x → 設定タブ
Brocade 8Gb ファイバチャネルスイッチモジュール，Brocade 8/16Gb ファイバチャネルスイッチモジュールおよび Brocade 16Gb ファイバチャネルスイッチモジュールの Web コンソールへのリンク	Resources タブ → Modules → 全モジュール → スイッチモジュール → スイッチモジュール x → 設定タブ
Hitachi ファイバチャネル拡張カード設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → I/O カードタブ

表 2-64 CLI コンソールでの操作方法

項目	コマンド
スイッチモジュールの CLI コンソールへのリンク	change console -s

2.9.2 サーバブレード(BMC 設定)

マネジメントモジュールから，BMC 設定の実施が可能です。

設定した項目は，即時反映されます。

設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

BMC 設定項目の中に資産管理タグがあります。資産管理タグを設定すると，次の項目で資産管理タグの内容が表示されます。

- マネジメントモジュールの Web コンソールの Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → ハードウェアタブ内にある「名称」欄
- HCSM に表示されるサーバ名

BS520H サーバブレード A1 に資産管理タグで「Server ABC」と設定した場合の表示例を示します。

Server ABC(BladeSymphony 520HA1)

参考 BS520A サーバブレード A1，BS540A サーバブレード A1/B1 では，資産管理タグの設定はサポートしていません。

2.9.3 サーバブレード(UEFI 設定)

マネジメントモジュールから，UEFI 設定の実施が可能です。

設定した項目は，次回のサーバブレード電源 ON 時に反映されます。

設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。

重要

- マネジメントモジュールから設定できない項目がありますので，その項目は，UEFI セットアップメニューから設定を実施してください。詳細は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」および「*BladeSymphony BS500 EFI ユーザーズガイド*」を参照してください。
- 設定変更後，サーバブレードの電源 ON を実施する前に N+M コールドスタンバイの切替が発生した場合，設定変更した値は破棄され，N+M コールドスタンバイで引き継いだデータで起動します。
- サーバブレードの電源 ON 後，OS が起動するまでの間に設定変更した場合，タイミングによっては設定が反映されない場合があります。設定変更は，サーバブレード電源 OFF 時もしくは OS 起動後に実施してください。

2.9.4 Hitachi LAN スイッチモジュールの設定

マネジメントモジュールから，スイッチモジュール設定の実施が可能です。設定した項目は，即時反映されます。

設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。

重要 マネジメントモジュールから設定できない項目がありますので，その項目は，スイッチモジュールのコンソールから設定を実施してください。詳細は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」およびスイッチモジュールのマニュアルを参照してください。

2.9.5 Hitachi ファイバチャネル拡張カードの設定

マネジメントモジュールから，拡張カード設定の実施が可能です。

設定した項目は，次回のサーバブレード電源 ON 時に反映されます。

設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。

重要 設定変更後，サーバブレードの電源 ON を実施する前に N+M コールドスタンバイの切替が発生した場合，設定変更した値は破棄され，N+M コールドスタンバイで引き継いだデータで起動します。

2.10 本装置における WWN，MAC アドレスについて

システム装置内の WWN および MAC アドレスについて説明します。

2.10.1 WWN，MAC アドレスの種別

本装置で使用可能な WWN，MAC アドレスには，次の 3 種類が存在します。

- original WWN / original MAC アドレス

  ファイバチャネル拡張カードや LAN 拡張カードが固有に持ち，書換え不可能な WWN，MAC アドレスです。

- additional WWN / additional MAC アドレス

  ファイバチャネル拡張カードや LAN 拡張カードに追加で割り当てる WWN，MAC アドレスです。これは書換え可能であり，BladeSymphony のみで使用する WWN，MAC アドレスです。ファイバチャネル拡張カードや LAN 拡張カードを交換しても，同じスロットに搭載する限りは，additional WWN，additional MAC アドレスが変わることはありません。そのため，拡張カードを交換した場合でも，ファイバチャネルスイッチモジュールや LAN スイッチモジュール，その他関連装置の設定を変更する必要がありません。

  additional WWN は，N+M コールドスタンバイ機能でも使用します。「2.10.5 N+M コールドスタンバイと WWN，MAC アドレスの関係」を参照してください。

- HVM で使用する WWN / MAC アドレス

  HVM が管理する WWN，MAC アドレスです。

  WWN については virtual FC WWN シード情報を元に，HVM システムごとにユニークになるように HVM が生成します。ファイバチャネル拡張カードを HVM モードで使用する場合は，PCI デバイス占有指定，共有指定に関わらず，本 WWN が使われます。

  また，ファイバチャネル拡張カードを交換しても，同じスロットに搭載する限り WWN が変わることはありません。

  MAC アドレスについては VNIC System No を元に，HVM システムごとにユニークになるように HVM が生成します。LAN 拡張カードを HVM モードで使用する場合は，PCI デバイス共有指定では，本 MAC アドレスが使われます。PCI デバイス占有指定では，Basic モードと同じ MAC アドレスが使われます。

  また，LAN 拡張カードを交換しても，PCI デバイス共有指定および PCI デバイス占有指定で additional MAC アドレスを使用する場合は，同じスロットに搭載する限り MAC アドレスが変わることはありません。

  ※詳細は「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

2.10.2 WWN，MAC アドレスの種別に関する注意事項

- Broadcom 1Gb LAN 拡張カードの additional MAC アドレス機能について

  BS520H サーバブレード A1/B1，BS520A サーバブレード A1，BS540A サーバブレード A1/B1 サーバブレードでは，サポートしていません。必ず original MAC アドレスを選択して運用してください。

- Emulex 8Gb 2 ポートファイバチャネル拡張カードの additional WWN 機能, original WWN 表示機能は，次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0115 以降

  サーバブレードファームウェア

  BS520H サーバブレード A1/B1 の場合は，統合ファームウェア 01-37 以降

- BS520H サーバブレード A1/B1/A2/B2，BS520A サーバブレード A1，BS540A サーバブレード A1/B1，の Emulex 10Gb CNA/LAN 拡張カード，オンボード CNA(2 ポート)の次の機能については，ファームウェアのバージョン，Personality 設定，MultiChannel Support 設定によって，「表 2-65 Personality 設定/MultiChannel Support 設定の制限事項」の(1)から(4)に示す制限があります。ご使用の際は，制限事項を守って使用してください。

  - MAC 機能

    additional MAC アドレスの割り当て機能

    マネジメントモジュールの MAC アドレス表示機能

  - WWN 機能

    additional WWN の割り当て機能

マネジメントモジュールの WWN 表示機能

表 2-65 Personality 設定/MultiChannel Support 設定の制限事項

Personality 設定	MultiChannel Support 設定			
	Disabled		Enabled	
	MAC	WWN	MAC	WWN
NIC(NIC Only)	制限なし	－ ※1	(1)	－ ※1
iSCSI(NIC+iSCSI)	(2)	－ ※1	(1)	－ ※1
FCoE(NIC+FCoE)	(3)	(4)	(1)/(3)	(4)

※1：Personality 設定が FCoE の場合のみ WWN は使用可能です。

「表 2-65 Personality 設定/MultiChannel Support 設定の制限事項」の(1)～(4)について，以下に示します。

- (1)MultiChannel Support 設定が Enable 時の additional MAC アドレス割り当て機能およびマネジメントモジュールの MAC アドレス表示機能は次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0125 以降

  サーバブレードファームウェア

  ・BS520H サーバブレード A1/B1 の場合は，統合ファームウェア 01-44 以降

  ・BS520A サーバブレード A1 の場合は，統合ファームウェア 02-16 以降

  ※MultiChannel Support 設定の詳細は，「*OneCommandManager ガイド*」を参照してください。

- (2)Personality 設定が iSCSI かつ MultiChannel Support 設定が Disabled 時の iSCSI ポートの additional MAC アドレスの割り当て機能は次に示す制限があります。

  ◦ BS520H サーバブレード A1/B1，BS520A サーバブレード A1，BS540A サーバブレード A1/B1 は非サポートです。

  ◦ BS520H サーバブレード A2/B2 では次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0165 以降

  サーバブレードファームウェア

  統合ファームウェア 04-11 以降

  非サポートファームウェアで additional MAC アドレスを選択して運用していた場合，サポートファームウェアを適用すると iSCSI ポートが additional MAC アドレスに変わってしまいます。

  このため，非サポートファームウェア使用時は，必ず original MAC アドレスを選択して運用してください。

- (3)FCoE ポートの additional MAC アドレス割り当て機能およびマネジメントモジュールの MAC アドレス表示機能は次に示す制限があります。

  ◦ BS520H サーバブレード A1/B1，BS520A サーバブレード A1，BS540A サーバブレード A1/B1 は非サポートです。

  ◦ BS520H サーバブレード A2/B2 では次に示すバージョンからサポートしています。

  マネジメントモジュール

A0165 以降

サーバブレードファームウェア

統合ファームウェア 04-11 以降

非サポートファームウェアで additional MAC を選択して運用していた場合，サポートファームウェアを適用すると FCoE ポートの MAC が additional MAC に変わってしまいます。

このため，非サポートファームウェア使用時は，必ず originalMAC を選択して運用してください。

- (4)FCoE ポートの additional WWN 割り当て機能およびマネジメントモジュールの WWN アドレス表示機能は次に示す制限があります。
  - BS520H サーバブレード A1/B1，BS520A サーバブレード A1，BS540A サーバブレード A1/B1 は非サポートです。
  - BS520H サーバブレード A2/B2 では次に示すバージョンからサポートしています。

    マネジメントモジュール

    A0165 以降

    サーバブレードファームウェア

    統合ファームウェア 04-11 以降

    非サポートファームウェアで additional WWN を選択して運用していた場合，サポートファームウェアを適用すると FCoE ポートの WWN が additional WWN に変わってしまいます。

    このため，非サポートファームウェア使用時は，必ず original WWN を選択して運用してください。

- BS520X サーバブレード B1 の Emulex 10Gb オンボード CNA(4 ポート)の以下機能は次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0220 以降

  サーバブレードファームウェア

  統合ファームウェア 06-12 以降

  - MAC 機能

    additional MAC アドレスの割り当て機能

    マネジメントモジュールの MAC アドレス表示機能
  - WWN 機能

    additional WWN の割り当て機能

    マネジメントモジュールの WWN 表示機能

  非サポートファームウェアで additional MAC アドレスを選択して運用していた場合，サポートファームウェアを適用すると MAC アドレスが additional MAC アドレスに変わってしまいます。このため，非サポートファームウェア使用時は，必ず original MAC アドレスを選択して運用してください。

  非サポートファームウェアで additional WWN を選択して運用していた場合，サポートファームウェアを適用すると FCoE ポートの WWN が additional WWN に変わってしまいます。 このため，非サポートファームウェア使用時は，必ず original WWN を選択して運用してください。

- Emulex 10Gb オンボード CNA(4 ポート)の Personality 設定で Custom を選択した場合は，additional MAC アドレス割り当ておよび additional WWN 割り当て機能を使用できません。このため，Custom を選択した場合は，必ず original MAC アドレスと original WWN を選択して運用してください。

2.10.3 Basic モードでの WWN，MAC アドレスの選択

Basic モードでは，使用する WWN，MAC アドレスを，additional，original から選択することができます。(以降，これを WWN 種別，MAC 種別と呼びます)

WWN 種別，MAC 種別の選択はサーバブレード単位で実施することができ，WWN 種別，MAC 種別それぞれで additional，original から選択可能です。WWN 種別，MAC 種別を変更すると，そのサーバブレードに搭載されているすべてのファイバチャネル拡張カードや LAN 拡張カードの値が切り替わります。

WWN 種別，MAC 種別は，次の理由から，additional を選択して運用することを推奨します。

- 拡張カードを交換しても WWN，MAC アドレスが変わらないので，拡張カード交換時の OS や外部機器への影響を最小限に抑えられます。

参考 SMP 構成のサーバブレードは，プライマリサーバブレードに指定された設定値で動作します。ノンプライマリサーバブレードに，プライマリサーバブレードと異なる設定値を指定しないでください。

表 2-66 Web コンソールでの操作方法

項目	画面
WWN 種別の表示，設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 設定タブ → サーバブレード設定
MAC 種別の表示，設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 設定タブ → サーバブレード設定

表 2-67 CLI コンソールでの操作方法

項目	コマンド
WWN 種別の表示	show blade setting
WWN 種別の設定	set blade preconf
MAC 種別の表示	show blade setting
MAC 種別の設定	set blade preconf

2.10.4 HVM モードでの WWN，MAC アドレスの選択

HVM モードでは，WWN 種別の設定によらず，HVM で使用する WWN が必ず使用されます。

PCI デバイス共有指定の場合は，MAC 種別の設定に拠らず，HVM で使用する MAC アドレスが必ず使用されます。PCI デバイス占有指定の場合は，MAC 種別に設定した MAC アドレスが使用されます。

2.10.5 N+M コールドスタンバイと WWN，MAC アドレスの関係

Basic モードで N+M コールドスタンバイを実行する場合，常に additional WWN を使用します。N+M 切り替え時には，現用サーバブレードに搭載したファイバチャネル拡張カードの additional WWN を予備サーバブレードのファイバチャネル拡張カードに設定することにより，SAN 接続を引き継ぎます。N+M コールドスタンバイでは，N+M 切り替えしてもサーバブレード上の OS からみ

た WWN が変更されないため，WWN に依存するソフトウェア機能（Persistent Binding など）がそのまま利用できます。

MAC アドレスについては，MAC 種別の設定に従い，original MAC アドレス，additional MAC アドレスを選択して使用可能です。additional MAC アドレスを選択した場合，N+M 切り替え時に MAC アドレスの値を引き継ぎます。そのため，N+M 切り替えしてもサーバブレード上の OS からみた MAC アドレスが変更されないため，MAC アドレスに依存した OS 設定などを実施することができます。

HVM モードで N+M コールドスタンバイを実行する場合，HVM で使用する WWN，MAC アドレスは N+M 切り替え時に引き継がれます。Basic モード同様，N+M 切り替えしてもサーバブレード上の OS からみた WWN，MAC アドレスは変更されないため，WWN，MAC アドレスに依存した機能を実施することができます。

2.10.6 additional WWN，additional MAC アドレスの初期化

N+M コールドスタンバイでは，additional WWN，additional MAC アドレスを別サーバブレードに引き継ぐことができます。しかし，何らかの要因でこれを元に戻す場合，マネジメントモジュールのコンソールから additional WWN，additional MAC アドレスの値を初期化（工場出荷時点の値に戻す），変更を実施することができます。

重要 通常は JP1/ServerConductor/Blade Server Manager からの N+M コールドスタンバイの切り戻し機能で元に戻すことを推奨します。JP1/ServerConductor/Blade Server Manager では元に戻せない場合のみ，本処理を実施するようにしてください。
※本処理を実施する場合，N+M コールドスタンバイの現用系，予備系両方で同時に実施し，WWN，MAC アドレスが重複しないよう十分注意して実施してください。

参考 SMP 構成の場合，サーバブレードの初期化は SMP を構成するすべてのサーバブレードで同時に実行されます。

表 2-68 Web コンソールでの操作方法

項目	画面
additional WWN の初期化	Resources タブ → Systems → WWN 管理 → 該当サーバブレードをクリック → 詳細表示 → Additional WWN → 初期設定
additional WWN の変更	Resources タブ → Systems → WWN 管理 → 該当サーバブレードをクリック → 詳細表示 → Additional WWN → 編集
additional MAC アドレスの初期化	Resources タブ → Systems → MAC 管理 → 該当サーバブレードをクリック → 詳細表示 → Additional MAC → 初期設定
additional MAC アドレスの変更	Resources タブ → Systems → MAC 管理 → 該当サーバブレードをクリック → 詳細表示 → Additional MAC → 編集

2.10.7 WWN，MAC アドレスの確認方法

マネジメントモジュールのコンソールからは，次のことを確認することができます。

- original WWN
- additional WWN
- 現在使用している WWN
- original MAC アドレス
- additional MAC アドレス
- 現在使用している MAC アドレス
- HVM で使用する WWN

・ HVM で使用する MAC アドレス

マネジメントモジュールからこれらの値を確認することで，サーバブレードの電源を投入し，OS 画面や UEFI 画面を確認しなくても，WWN，MAC アドレスの値を確認することができます。

また，サーバブレードに搭載されている拡張カードの WWN，MAC アドレスの一括表示が可能なため，使用している WWN，MAC アドレスを一目で確認することができます。(※1)

※1：マネジメントモジュールから変更した WWN，MAC アドレスは，次回サーバブレードの電源投入時に，実際のファイバチャネル拡張カードや LAN 拡張カードに設定されます。このため，WWN，MAC アドレスを変更してからサーバブレードの電源投入を行っていない場合，マネジメントモジュールのコンソールに表示される「現在使用している WWN」，「現在使用している MAC アドレス」は，実際のファイバチャネル拡張カードや LAN 拡張カードに割り当てられている値と異なる場合があります。

表 2-69 Web コンソールでの操作方法

項目	画面
original WWN の値の表示	Resources タブ → Systems → WWN 管理 → 該当サーバブレードをクリック → 詳細表示 → Original WWN
additional WWN の値の表示	Resources タブ → Systems → WWN 管理 → 該当サーバブレードをクリック → 詳細表示 → Additional WWN
現在使用している WWN の値の表示	Resources タブ → Systems → WWN 管理 → Current WWN 表示
original MAC アドレスの値の表示	Resources タブ → Systems → MAC 管理 → 該当サーバブレードをクリック → 詳細表示 → Original MAC
additional MAC アドレスの値の表示	Resources タブ → Systems → MAC 管理 → 該当サーバブレードをクリック → 詳細表示 → Additional MAC
現在使用している MAC アドレスの値の表示	Resources タブ → Systems → MAC 管理 → Current MAC 表示
HVM で使用する WWN の値の表示	Resources タブ → Systems → WWN 管理 → 該当サーバブレードをクリック → 詳細表示 → Virtual WWN
HVM で使用する MAC アドレスの値の表示	Resources タブ → Systems → MAC 管理 → 該当サーバブレードをクリック → 詳細表示 → Virtual MAC

重要 Emulex 8Gb 2 ポートファイバチャネル拡張カードの original WWN 表示機能が未サポートの場合，original WWN の値は表示されません。BIOS 設定画面から確認してください。

表 2-70 CLI コンソールでの操作方法

項目	コマンド
original WWN の値の表示	show wwn original
現在使用している WWN の値の表示	show wwn current
original MAC アドレスの値の表示	show mac original
現在使用している MAC アドレスの値の表示	show mac current

参考 Emulex 10Gb CNA 拡張カードまたはオンボード CNA の場合，Web コンソールまたは，CLI コンソールで表示される WWN は次のようになります。

表 2-71 Emulex 10Gb CNA 拡張カードまたはオンボード CNA(2 ポート)の場合

ポート	World Wide Port Name	World Wide Node Name
0	コントローラ 0 のポート 0 の World Wide Port Name	コントローラ 0 のポート 0 の World Wide Node Name
1	コントローラ 0 のポート 1 の World Wide Port Name	コントローラ 0 のポート 1 の World Wide Node Name
2	コントローラ 1 のポート 0 の World Wide Port Name	コントローラ 1 のポート 0 の World Wide Node Name
3	コントローラ 1 のポート 1 の World Wide Port Name	コントローラ 1 のポート 1 の World Wide Node Name

表 2-72 Emulex 10Gb オンボード CNA(4 ポート)の場合

ポート	World Wide Port Name	World Wide Node Name
0	コントローラ 0 のポート 0 の World Wide Port Name	コントローラ 0 のポート 0 の World Wide Node Name
1	コントローラ 0 のポート 1 の World Wide Port Name	コントローラ 0 のポート 1 の World Wide Node Name
2	コントローラ 0 のポート 2 の World Wide Port Name	コントローラ 0 のポート 2 の World Wide Node Name
3	コントローラ 0 のポート 3 の World Wide Port Name	コントローラ 0 のポート 3 の World Wide Node Name

※1：オンボード CNA(2 ポート)はコントローラを 1 つしか持っていないため，Current WWN，Original WWN はポート 0 とポート 1 のみ表示されます。

※2：Emulex 10Gb CNA 拡張カードまたはオンボード CNA 内のコントローラの Personality 設定が FCoE でない場合，Current WWN，Original WWN は表示できません。

その場合，以下のメッセージが出力されます。

＜ Web コンソール＞

「カード未搭載　WWN 情報が存在しません」

＜ CLI コンソール＞

「WWN information does not exist」

2.10.8 additional WWN，additional MAC アドレスの変更ログ

N+M コールドスタンバイでの additional WWN, additional MAC アドレスの引継ぎや, additional WWN，additional MAC アドレスの初期化，設定変更の履歴は，マネジメントモジュール内で WWN，MAC アドレスでそれぞれ 1023 回の変更分記録されており，マネジメントモジュールのコンソールからその変更ログを確認することができます。

変更ログには，時刻と変更前後の値に加えて，変更契機（N+M コールドスタンバイの切り替えによるものか，マネジメントモジュールのコンソールからによるものか）も残るので，どの時刻に N+M コールドスタンバイの切り替えが発生し，WWN や MAC アドレスがどの値に変化したのかを知ることができます。

WWN，MAC アドレスの変更ログが確認できるのは，additional WWN，additional MAC のみで，HVM が使用する WWN，MAC アドレスについては，変更ログを確認することができません。

表 2-73 Web コンソールでの操作方法

項目	画面
WWN 変更ログの表示	Alerts タブ → Additional WWN 変更ログ
MAC アドレス変更ログの表示	Alerts タブ → Additional MAC 変更ログ

表 2-74 CLI コンソールでの操作方法

項目	コマンド
WWN 変更ログの表示	show log wwn-edit
MAC アドレス変更ログの表示	show log mac-edit

2.11 ホスト情報の表示

ServerNavigator は，サーバの OS/ドライバの自動インストールや，ユーティリティ/ドライバ/ファームウェアの自動アップデート機能を提供するサーバに添付しているツールキットです。ServerNavigator をサーバブレードの OS にインストールすると，マネジメントモジュールの Web コンソールで，OS の情報(ホスト情報)を確認することができます。ServerNavigator のインストールまたはバージョンアップの方法は，「*Hitachi Server Navigator ユーザーズガイド*」を参照してください。マネジメントモジュールの Web コンソールで，表示可能ホスト情報は以下の通りです。

表 2-75 表示可能ホスト情報

情報	説明	Windows	Linux
OS ※1	サーバの OS 種別	Windows バージョン+サービスパックバージョン 表示例：Microsoft Windows Server 2008 Standard Service Pack 2	/etc/redhat-release の中身を表示 表示例：Red Hat Enterprise Linux Server release 5.7 (Tikanga)
ホスト名 ※2	サーバの OS に設定されているホスト名	コンピュータ名	hostname コマンドの内容を表示

※1：OS の名称に特殊文字がある場合，Web コンソールでの表示では除外して表示します。

※2：ホスト名を設定する際は，半角英数記号を使用してください。半角英数記号以外の文字を設定した場合，Web コンソールでホスト名が正しく表示されません。

重要

- ホスト情報の表示は，OS に ServerNavigator がインストールされていないと，表示されません。
- ホスト情報の表示は，Windows と Linux と VMWare のみでサポートしています。
- 仮想環境(Hyper-V，HVM，VMware，等)のゲスト OS のホスト情報の表示は非サポートです。
- ホスト情報の表示は，次に示すバージョンからサポートしています。

  マネジメントモジュール

  A0150 以降

  サーバブレードファームウェア

  ・BS520H サーバブレード A1/B1 の場合は，統合ファームウェア 01-60 以降
  ・BS520A サーバブレード A1 の場合は，統合ファームウェア 02-30 以降
  ・BS540A サーバブレード A1/B1 の場合は，統合ファームウェア 03-10 以降
  ・上記以外のサーバブレードは，統合ファームウェア全バージョンでサポートしています。

  ServerNavigator

X.3.3.4（但し，ESXi は 4.3.3.3）以降

※ファームウェアが一つでもサポートバージョンより古い場合，ホスト情報は「-----」と表示されます。

ホスト情報は，OS 起動後 Server Navigator が自動起動したタイミングでサーバブレード上に保存されます。ホスト名の変更をしたときは，Web コンソールの表示は自動で反映されないので，反映させたいときは OS を再起動してください。

OS をシャットダウンしても，サーバブレード上に保存されたホスト情報は残ります。OS に ServerNavigator をインストールし，ホスト情報を表示させていた場合に，以下を実施した際は，実際の OS 情報と表示されているホスト情報に違いが生じる可能性があります。

- ServerNavigator をアンインストールした場合
- OS をアンインストールし，ServerNavigator サポートの OS をインストールし，ServerNavigator はインストールしなかった場合
- OS をアンインストールし，ServerNavigator 非サポートの OS をインストールした場合

  この場合は，サーバブレード上に保存されたホスト情報を削除してください。ホスト情報の削除は，マネジメントモジュールの Web コンソールで実施可能です。

参考 ホスト情報の削除は，サーバブレードの電源状態が OFF 状態のときのみ可能です。

表 2-76 Web コンソールでの操作方法

項目	画面
ホスト情報の表示	Resources タブ → Modules → サーバブレード → サーバブレード x → Hosts タブ
ホスト情報の削除	Resources タブ → Modules → サーバブレード → サーバブレード x → Hosts タブ → ホスト情報クリア

N+M コールドスタンバイ構成時，現用系サーバブレードに ServerNavigator をインストールしていた場合に，N+M コールドスタンバイの切り替えが発生すると，予備系サーバブレードで ServerNavigator が起動し，予備系サーバブレードにホスト情報が保存されます。その後，現用系サーバブレードに N+M コールドスタンバイの復帰をしても，予備系サーバブレードにホスト情報は保存されたままとなります。この際も，ホスト情報の削除の機能を使用することで，予備系サーバブレードのホスト情報を削除することが可能です。

2.12 JP1/ServerConductor/Blade Server Manager 連携

マネジメントモジュールと JP1/ServerConductor/Blade Server Manager の連携について説明します。

2.12.1 通知先 BSM の設定

JP1/ServerConductor/Blade Server Manager(以下 BSM)は，複数のサーバを一元管理するためのソフトウェアです。BSM を使用して本システム装置を管理することで，システム管理の効率化を実現できます。BSM を使用して本システム装置を管理する場合，マネジメントモジュールへの通知先 BSM の設定が必要となります。設定項目は次のとおりです。設定内容については「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。なお，通知先 BSM は計 4 つ設定可能です。

重要 通知先 BSM の設定は，シャーシ ID の設定を行った後に実施してください。
通知先 BSM の設定後にシャーシ ID を変更する場合，BSM にて，ホスト，HVM，サーバシャーシの削除および再登録が必要です。詳細は BSM のマニュアルを参照してください。
通知先 BSM の設定後にシャーシ ID を変更した場合，変更前のシャーシ ID の情報が BSM 上に残ってしまい，BSM でのシャーシ管理が正しく行えない場合があります。

通知先 BSM の設定項目

通知先 BSM の設定項目は次の 3 項目です。

- 通知先 BSM 名称
- IP アドレス
- アラートレベル

また，詳細設定では次の情報を変更することも可能です。通常はこれらの設定は変更不要です。設定内容については「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

通知先 BSM の詳細設定項目

通知先 BSM の詳細設定項目は次の 4 項目です。

- コマンドポート番号
- アラートポート番号
- アラート接続リトライ間隔
- アラート接続リトライ継続時間

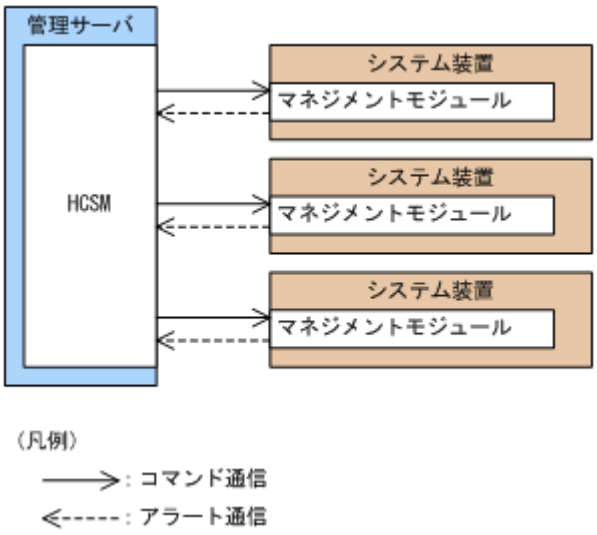
重要 アラートポート番号をデフォルト(20079)から変更した場合は, BSM 側 service ファイルの設定変更が必要です。詳細は BSM のマニュアルを参照してください。

表 2-77 Web コンソールでの操作方法

項目	画面
通知先 BSM の表示，設定	Administration タブ → JP1/SC/BSM 連携 → Action → ポート番号設定

2.13 HCSM 連携

Hitachi Compute Systems Manager(以下 HCSM)は, 大規模システムにおけるシステム装置の運用機能を提供することを目的としたソフトウェアです。システム管理者は，HCSM を利用することにより，システム内のハードウェア資源の管理，稼働状態の監視，N+M コールドスタンバイ，電力管理，ハードウェアの操作を行うことができます。HCSM とマネジメントモジュールは相互に通信することで，システム管理者に管理機能を提供します。HCSM とマネジメントモジュールは，2 つの通信路を確立します。



コマンド通信

HCSM がマネジメントモジュールに処理を要求する際に用います。

本通信では，HTTPS プロトコルを利用することで，通信内容の盗聴，改ざんを防ぎます。

アラート通信

マネジメントモジュールがシステム装置内で発生した事象を HCSM に通知する際に用います。

本通信では，SSL/TLS プロトコルを利用することで，通信内容の盗聴，改ざんを防ぎます。

マネジメントモジュールは，最大 4 台までの HCSM と連携することができます。

参考

- HCSM と連携する場合, HTTPS を有効にする必要があります。HTTPS 設定の確認および設定変更は,「2.4 セキュリティ」を参照してください。
- セキュリティ強度を"高"に設定した場合，あるいはセキュリティ強度を"通常"に設定した状態で TLS1.2 以外での通信を不可と設定した場合，TLS1.2 に非対応の HCSM とは接続できません。HCSM を使用する際に必要な手順は，HCSM の取扱説明書，マニュアルを参照してください。
- HCSM の設定で，HTTPS 通信を行う際に利用するポート番号を 443 から変更されている場合，マネジメントモジュールの利用するポート番号も HCSM と合わせてください。マネジメントモジュールの利用するポート番号を変更する際は，サービスの HTTPS のポート番号を変更してください。

2.13.1 HCSM からのディスカバリについて

HCSM は，管理対象となるネットワークに存在するシステム装置を検索する機能(以下ディスカバリ)を有しています。

システム管理者は，HCSM のユーザインタフェースからディスカバリを実行することで，ネットワークに存在するシステム装置を一括で管理対象にすることができます。HCSM は，システム装置を管理対象に設定した際に，当該システム装置のマネジメントモジュールに自身の情報を登録します。

ディスカバリによってマネジメントモジュールに登録された HCSM の情報は，Web コンソールおよび CLI コンソールで確認することができます。

参考 マネジメントモジュールに 4 台の HCSM が登録されている状態で，登録されている HCSM とは別の HCSM 上でディスカバリを実行した場合，当該マネジメントモジュールが登録されているシステム装置は，管理対象とはなりません。

表 2-78 Web コンソールでの操作方法

項目	画面
HCSM の情報の表示，設定	Administration タブ → HCSM 連携

表 2-79 CLI コンソールでの操作方法

項目	コマンド
HCSM の情報の表示	show hcsm setting
HCSM の情報の変更	set hcsm manager
HCSM の情報の削除	delete hcsm manager

2.13.2 HCSM 連携のオプション設定

HCSM との連携に関して事前にマネジメントモジュールに設定する必要はなく，システム装置出荷時の設定状態のまま HCSM のユーザインタフェースからディスカバリを実行することで，マネジメントモジュールは，HCSM と連携することができます。本項では，HCSM との連携に関するオプション設定について示します。

- HCSM からの管理を抑止する

  HCSM 連携機能を無効にすることができます。

  本設定を行うことで，HCSM から当該システム装置管理させなくできます。

  無効にした状態で，HCSM からディスカバリを実行した場合，当該システム装置は管理対象になりません。

- IP アドレスによる接続制限を行う

  接続制限を有効にすることで，マネジメントモジュールに登録された HCSM サーバのみと連携させることができます。

  接続制限が有効な状態で，登録外の HCSM からディスカバリを実行した場合，当該システム装置は管理対象になりません。

  本設定を利用することで，システム構築後に不当に設置された HCSM の管理対象となることを防ぐことができます。

参考 接続制限を有効の状態で，新たな HCSM から当該システム装置を管理する場合は，ディスカバリを実行する前に，マネジメントモジュールに IP アドレスを登録する必要があります。

- 認証用のアカウント/パスワードを設定する

  マネジメントモジュールは，HCSM と連携を行う際に，アカウントとパスワードによる認証を行います。

  マネジメントモジュールおよび HCSM は，共通のデフォルトアカウント/パスワードを持っています。デフォルトのアカウント/パスワードの代わりに，システム管理者が指定したアカウント/パスワードで認証を行うことができます。

  認証用のアカウント/パスワードを指定する場合，マネジメントモジュールと HCSM にはそれぞれ同じアカウント/パスワードを指定してください。マネジメントモジュールと HCSM のそれぞれで使用するアカウント/パスワードが一致しないと，認証に失敗し HCSM と連携できなくなります。

重要 マネジメントモジュールファームウェアバージョン A0270 より前のバージョンでは HCSM に通知するアラートについての設定を変更可能となっていますが、Web コンソールや CLI コンソールを使ってこれらの設定を変更しないでください。
設定値を変更しても，HCSM 側でディスカバリを実行すると HCSM が持っている設定値に更新されます。
HCSM に通知するアラートについての設定項目と HCSM が持っているデフォルト値を次に示します。

- アラート送信先のポート番号：22611

- アラートレベル：情報と警告と障害
- リトライ間隔：2 分
- リトライ継続：10 分

表 2-80 Web コンソールでの操作方法

項目	画面
HCSM 連携のオプション設定の表示，設定	Administration タブ → HCSM 連携

表 2-81 CLI コンソールでの操作方法

項目	コマンド
HCSM 連携のオプション設定の表示	show hcsm setting
HCSM 管理の抑止設定の変更，接続制限設定の変更	set hcsm agent
HCSM の IP アドレスの設定	set hcsm manager
登録されている HCSM の情報の削除	delete hcsm manager

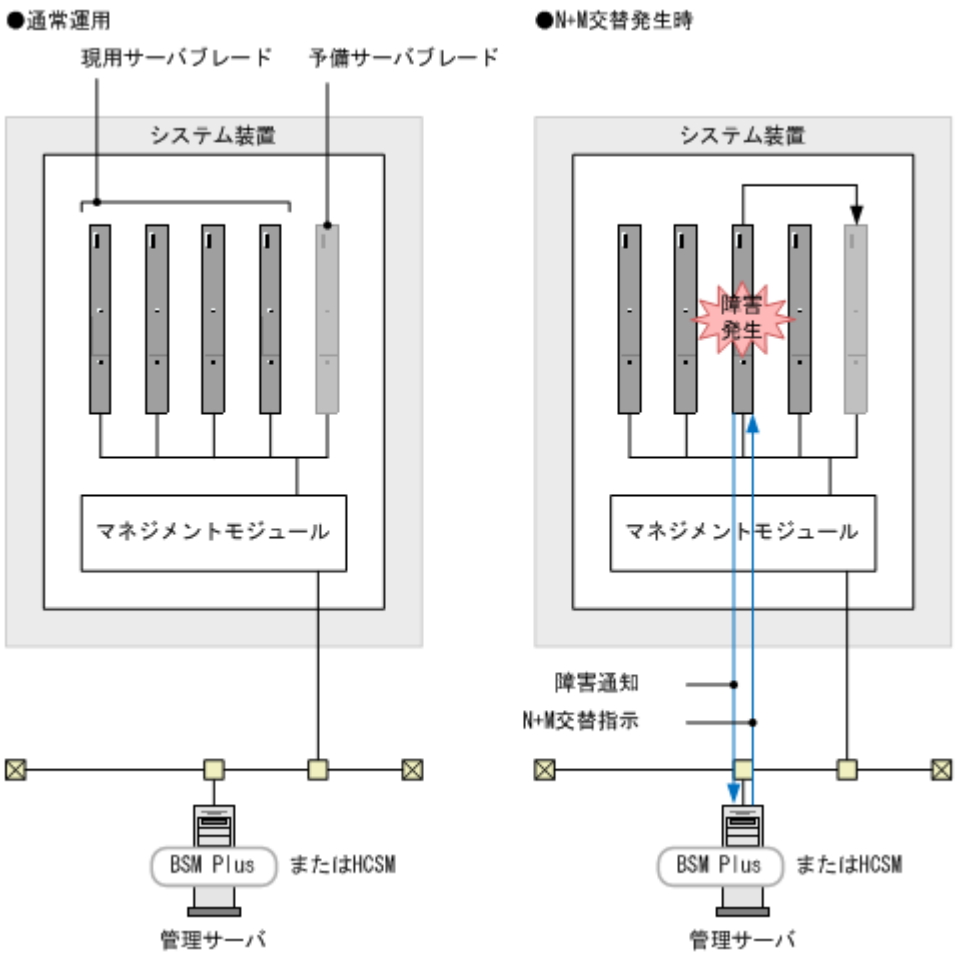
2.14 N+M コールドスタンバイ

N+M コールドスタンバイ機能について説明します。

2.14.1 N+M コールドスタンバイ概要

N+M コールドスタンバイ機能は，サーバブレードでハードウェア障害が発生した場合に，その障害通知を管理サーバ JP1/ServerConductor/Blade Server Manager Plus（以下 BSM Plus）または Hitachi Compute Systems Manager（以下 HCSM）で受け取り，障害を解析し，現用サーバブレード（業務サーバブレード）を予備サーバブレードに切り替える機能です。複数の現用サーバブレードに対して，予備サーバブレードを用意し，その予備サーバブレードを起動して業務を再開できます。ハードウェア障害によって運用は一時的に中断しますが, 少ないハードウェアリソースで, ハードウェア障害発生から運用再開までの障害対応を省力化できます。

N+M コールドスタンバイ機能は HVM にも対応しており，複数の LPAR が稼働している現用サーバブレードでハードウェア障害が発生した場合は，現用サーバブレード上で稼働していた LPAR を予備サーバブレード上で起動し直します。また，Basic モードの現用サーバブレードと HVM モードの現用サーバブレード間で予備サーバブレードを共用することもできます。



重要

- 現用サーバブレードと予備サーバブレードは，ハードウェア構成が同一である必要があります。同一サーバブレードモデル間の N+M コールドスタンバイのみ対応しています。
- HVM のライセンスには，Essential ライセンスや Advanced ライセンスなどがありますが，現用サーバブレードが Advanced ライセンス（Advanced モデル）の場合，予備サーバブレードにも Advanced ライセンスが必要です。現用サーバブレードと予備サーバブレードは，同じライセンスにしておいてください。
- Emulex 製ネットワーク製品(LAN/コンバージドネットワーク)を予備サーバブレードにご使用になる場合は，ファームウェアバージョンを最新にアップデートした構成で使用してください。

  最新のファームウェアは，「統合サービスプラットフォーム BladeSymphony の（サポート＆ダウンロード)」に掲載のファームウェアページをご確認ください。本ページに現在ご使用のファームウェアバージョンの確認方法も記入されています。
- 複数のサーバシャーシ構成で N+M コールドスタンバイを構築する場合，スイッチモジュールのハードウェア構成も同一にしてください。特に，現用サーバブレードが搭載されたサーバシャーシで 10Gb LAN スイッチモジュール，予備サーバブレードが搭載されたサーバシャーシで 1Gb LAN スイッチモジュールを搭載している場合，N+M 切替前後で LAN の帯域が変更され，ネットワークの性能低下など，OS 上の動作に影響を与える可能性があります。
- N+M 復帰を行う際，予備サーバブレードの動作モード(HVM モード/Basic モード)は，N+M グループ登録時の現用サーバブレードと同一でなければなりません。N+M 切り替え後に予備サーバブレードの動作モードを変更した場合は，必ず予備サーバブレードの動作モードを元に戻してから N+M 復帰を実行してください。N+M 切り替え後に予備サーバブレードの動作モードを変更したまま, N+M 復帰を実行すると次の事象が発生する場合があります。

  - HVM の構成情報が正しく復帰されないことがある

  - N+M 復帰に失敗することがある
- Emulex 10Gb CNA 拡張カードまたはオンボード CNA(2 ポート/4 ポート)の Personality 設定を FCoE とした N+M コールドスタンバイは非サポートです。

- Emulex 10Gb オンボード CNA(4 ポート)を有効とした N+M コールドスタンバイのサポート機能は，ファームウェアバージョンによって異なります。サポート機能は，「2.14.5 N+M コールドスタンバイの前提条件」を参照してください。
- HCSM バージョン 8.1.1 以降では，IPv6 ネットワークで接続することができます。ただし，複数のサーバシャーシ構成で N+M コールドスタンバイを構築する場合，HCSM との接続は，IPv4 ネットワークか IPv6 ネットワークのどちらかに揃えてご使用ください。

参考

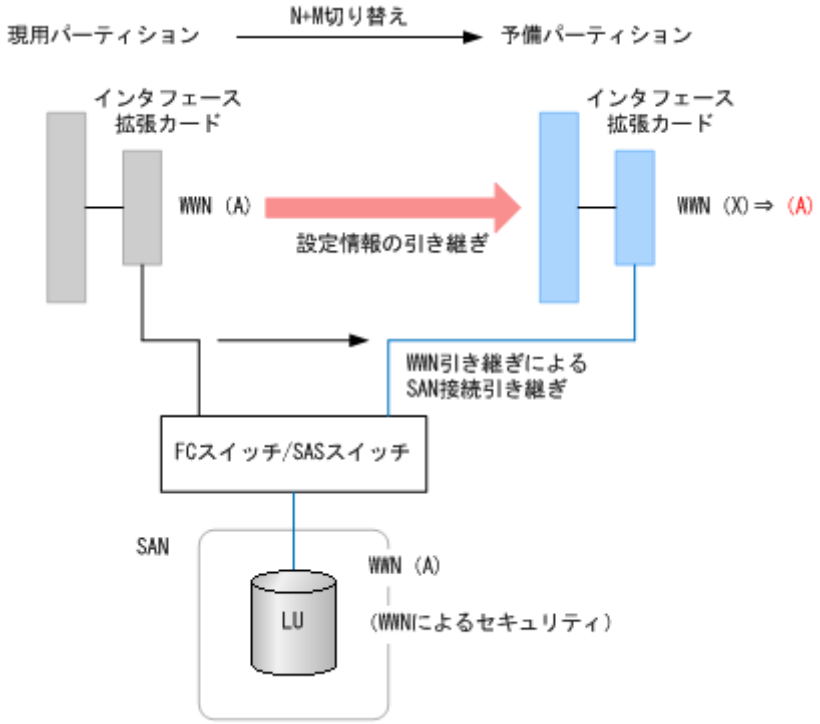
- 複数のシステム装置にわたり N+M コールドスタンバイを設定することができます。
- 現用サーバブレードと予備サーバブレードが同一システム装置内に存在する必要はありません。
- N+M コールドスタンバイの構築には，別途 JP1/ServerConductor/Blade Server Manager Plus または HCSM の導入が必要です。詳細は，弊社担当営業にお問い合わせください。
- HCSM で N+M コールドスタンバイをサポートする構成については，「HCSM サポートマトリクス」を参照してください。
- ウォッチドッグタイムアウトを契機に予備サーバブレードに切り替える場合は，マネジメントモジュールへの設定が必要です。

2.14.2 N+M コールドスタンバイの仕組み

N+M コールドスタンバイの仕組みを説明します。

(1) Basic モードのサーバブレードの場合

N+M コールドスタンバイでは，Basic モードサーバブレードの N+M 切り替えの際，現用サーバブレードの各種設定を予備サーバブレードに引き継ぎます。これによりサーバブレードが切り替えられても同一のディスク（LU）からサーバブレードを起動し，予備サーバブレードで現用サーバブレードと同じ OS 環境を再開することが可能となります。以降，これら引き継ぐ設定内容を「サーバブレードの設定情報」，または「設定情報」と呼びます。

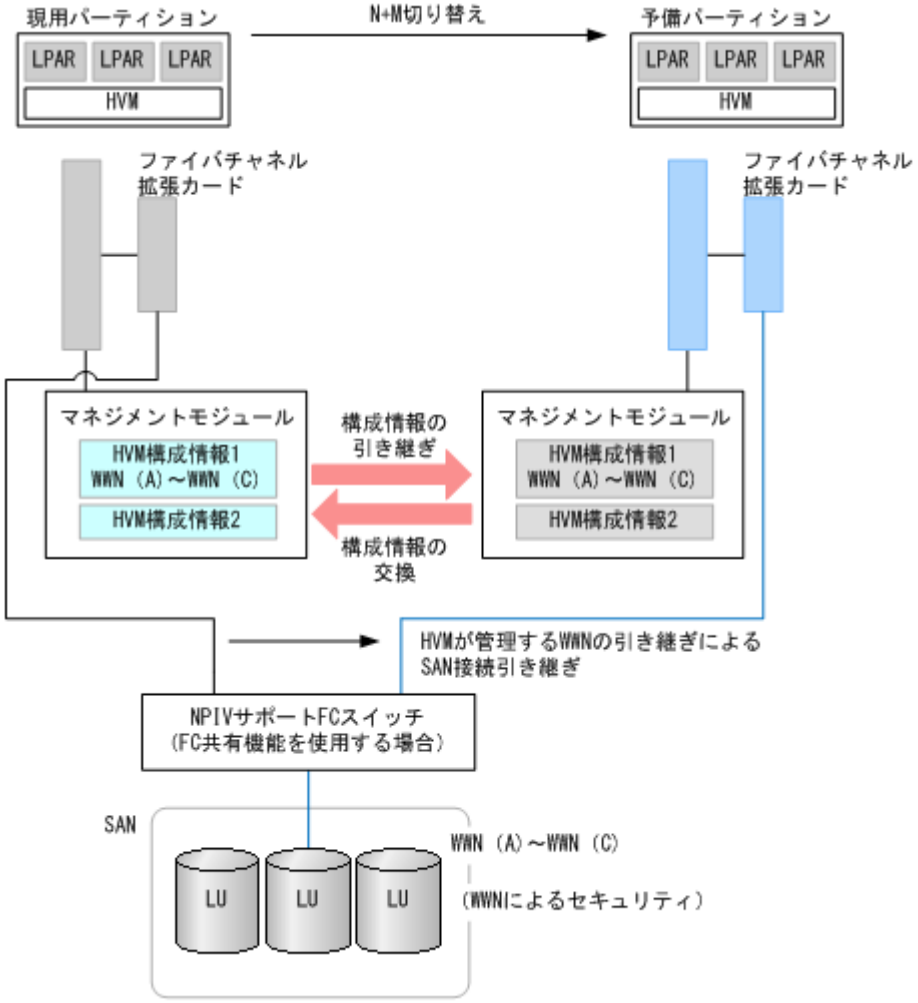


重要 「2.14.5 N+M コールドスタンバイの前提条件」の制限事項を確認してください

参考 現用サーバブレードと予備サーバブレードはハードウェア構成，インストールされるファームウェアのバージョンが同一である必要があります。

(2) HVM モードのサーバブレードの場合

N+M コールドスタンバイでは，HVM モードサーバブレードの N+M 切り替えの際，現用サーバブレードの HVM 構成情報（LPAR 設定，LPAR 状態，HVM が管理する WWN 情報など）を予備サーバブレードに複製し引き継ぎ，予備サーバブレードを HVM モードで起動します。これによりサーバブレードが切り替えられても，予備サーバブレードで現用サーバブレードと同一の LPAR 構成を再現することが可能となります。また，各 LPAR は現用サーバブレードと同じディスク（LU）から起動され OS 環境を再開できます。以降，これら引き継ぐ設定内容を「HVM 構成情報」，または「構成情報」と呼びます。



重要 必ず現用サーバブレードと予備サーバブレードで HVM ファームウェアのバージョンを同一にしてください。HVM ファームウェアのバージョンが異なる場合，N+M 切り替えに失敗する可能性があります。「2.14.5 N+M コールドスタンバイの前提条件」の制限事項を確認してください。

参考

- 予備サーバブレードへの切り替え契機は，現用サーバブレードのハードウェア障害です。
- Basic モードと同様，現用サーバブレードと予備サーバブレードはハードウェア構成，インストールされるファームウェアのバージョンが同一である必要があります。

2.14.3 N+M コールドスタンバイで引き継ぐサーバブレードの設定情報

N+M コールドスタンバイで引き継ぐサーバブレードの設定情報を説明します。

(1) BASIC モードのサーバブレードの場合

表 2-82 引き継ぎ区分と項目

区分	項目	備考
WWN	World Wide Node Name	※1
	World Wide Port Name	
MAC	Media Access Control address	※2
	MAC 種別	※3
サーバブレード設定(UEFI/BMC)※10	BMC 時刻の時刻合わせ方式，タイムゾーン設定	−
	スケジュールデータ	−
	EFI 設定	※4
	ブートオーダ	−
ファイバチャネル拡張カードの HBA BIOS 設定	HBA BIOS 有効無効設定	※5
	ブートプライオリティ有効無効設定	
	ブートターゲット WWN	
	ブートターゲット LUN	
Emulex 10Gb CNA/LAN 拡張カード，オンボード CNA(2 ポート/4 ポート)の設定	PXE ブート設定※11	※6
	VLAN 情報設定※11	
	ポート分割時の帯域設定	
	SR-IOV（MultiChannel Support 設定が Disabled の場合）	
	iSCSI 設定	
サーバブレード設定(SVP)	電源制御連動設定	※7
	N+M コールドスタンバイ支援機能設定	※8
	OS 種類（HVM 使用有無）	−
HA モニタ設定	HA モニタシステム名	※9
	HA モニタポート番号	
	HA モニタ N+M コールドスタンバイ支援機能設定	

※1

additional WWN を引き継ぎます。詳細は「2.10 本装置における WWN，MAC アドレスについて」を参照してください。

※2

additional MAC アドレスを引き継ぎます。詳細は「2.10 本装置における WWN，MAC アドレスについて」を参照してください。

※3

MAC 種別に設定された MAC アドレスを使用します。詳細は「2.10.3 Basic モードでの WWN，MAC アドレスの選択」を参照してください。

※4

マネジメントモジュールの Web コンソールの UEFI 設定にある項目のみ引き継ぎます。詳細は「2.9.3 サーバブレード(UEFI 設定)」を参照してください。

※5

Emulex 8Gb 2 ポートファイバチャネル拡張カードおよび Emulex 16Gb 2 ポートファイバチャネル拡張カードの場合は，セットアップメニューの全項目を引き継ぎます。

※6

現用系，待機系の Personality 設定が FCoE 以外であること，また MultiChannel Support 設定が同一であることが条件となります。Emulex 10Gb CNA 拡張カードまたはオンボード CNA(2 ポート/4 ポート)の Personality 設定を FCoE とした N+M コールドスタンバイは非サポートです。オンボード CNA(4 ポート)の場合，Personality 設定を iSCSI とした N+M コールドスタンバイは非サポートです。項目の詳細については，次のマニュアルを参照してください。

- *BladeSymphony Emulex 製アダプタ ユーザーズガイド ドライバ編*
- *BladeSymphony Emulex 製アダプタ ユーザーズガイド ハードウェア編*
- *BladeSymphony Emulex 製アダプタ ユーザーズガイド ユーティリティ編*

※7

詳細は「2.6.5 電源復旧時のサーバブレード動作設定」を参照してください。

※8

詳細は「2.14.11 N+M コールドスタンバイ構築手順」を参照してください。

※9

詳細は「2.15 HA モニタ連携」を参照してください。

※10

SMP 構成の場合，プライマリサーバブレードの設定情報だけが引き継がれます。

※11

オンボード CNA(4 ポート)の場合，この項目は引き継ぎません。

参考

- N+M 復帰時は，予備サーバブレードに引き継いだ情報を現用サーバブレードに戻すため，現用サーバブレードは N+M 切り替え前の状態に戻りますが，予備サーバブレードの情報は引き継いだ現用サーバブレードの情報のままになり，切り替え前の状態には戻りません。(ただし，WWN/MAC アドレスに関しては予備サーバブレードも切り替え前の状態に戻ります)
- Emulex 10Gb CNA を Personality:iSCSI で使用している場合，N+M 切替時の現用サーバブレードおよび N+M 復帰時の予備サーバブレードにおいて，iSCSI Initiator の IP Address および SubnetMask が 0 クリアされます。

(2) HVM モードのサーバブレードの場合

N+M コールドスタンバイでは，HVM モードの N+M 切り替え時に，「(1) BASIC モードのサーバブレードの場合」の情報と，次の HVM 構成情報を現用サーバブレードから予備サーバブレードに引き継ぎます。

表 2-83 引き継ぎ区分と項目

区分	項目	備考
LPAR 情報	LPAR 構成情報	—
	論理 NVRAM 情報	※1
	論理スケジュールデータ情報	—
HVM システム情報	システム構成情報	—
	PCI デバイス構成情報	—
	仮想 NIC 構成情報	—
	共有 FC 情報	—
	virtual FC WWN シード情報	—

※1：論理 UEFI のブートパス，オーダ，ブートタイマ，ドライバパス，オーダが格納されています。また，ドライバパスについては UEFI シェルから手動で追加した設定は引き継ぐことができません。

2.14.4 N+M 切り替え時間について

サーバブレード障害時の N+M 切り替えに必要な時間は次のとおりです。

(1) Basic モードサーバブレードの場合

N+M 切り替え時間 ＝
[切り替え開始待ち時間] ＋ [切り替え中の時間] ＋ [OS 起動時間]

(2) HVM モードサーバブレードの場合

N+M 切り替え時間 ＝
[切り替え開始待ち時間] ＋ [切り替え中の時間] ＋ [HVM 起動時間(※1)] ＋ [LPAR 上の OS 起動時間]

※1：5～10 分

参考 HCSM を用いた N+M コールドスタンバイ環境での切り替えにおいて，HCSM は切り替え後の予備系の OS 起動完了を監視しています。
HCSM は，ユーザが指定した「OS 起動完了までの最大待ち時間」内に予備系の OS が起動完了しない場合，予備系の OS が起動完了したかしなかったかに関わらず，HCSM のタスク結果表示画面に N+M 切り替え失敗のメッセージ(KASV00212-E)を表示します。このため，N+M 切り替えおよび予備系の OS 起動が完了した場合においても HCSM のタスク結果表示画面に N+M 切り替え失敗のメッセージ(KASV00212-E)が表示されることがあります。
サーバブレードの構成によっては(BS540A サーバブレード構成，SMP 構成など)，予備系の OS 起動完了までの時間が長くなるため，「OS 起動完了までの最大待ち時間」は適切な値を設定してください。

2.14.5 N+M コールドスタンバイの前提条件

N+M コールドスタンバイは次に示す装置の構成を前提条件とします。

- SAN ブートであること。
- 現用サーバブレード，予備サーバブレードのハードウェア構成が等価であること。
  - CPU 種，CPU 数
  - 搭載メモリ量
  - 拡張カード，I/O ボードモジュール（種別，サーバブレードからみた相対スロット位置）

参考 予備サーバブレードと現用サーバブレードで CPU 種，CPU 数，搭載メモリ量が異なって いても切り替えは可能ですが，事前切り替えテストにより予備サーバブレードで稼働できていることを確認してください。

- 現用サーバブレード，予備サーバブレードに拡張ブレード（PCI 拡張，ストレージ拡張）が接続されていないこと。
- 内蔵 HDD が搭載されていないこと。
- N+M グループ内では，異なるサーバブレードモデルを混在させないこと。
  (例：BS520A サーバブレード A1 と BS520H サーバブレード A1 の混在，BS520H サーバブレード A1 と BS520H サーバブレード B1 の混在など)
- HVM モードで N+M コールドスタンバイを構成する場合は，サーバブレードおよび周辺機器が HVM に対応していること。

- HVM モードで N+M コールドスタンバイを構成する場合は，現用サーバブレード，予備サーバブレードで使用するすべてのファームウェア(マネジメントモジュールファームウェア，サーバブレードファームウェア，HVM ファームウェア)が一致していること。
- HVM モードで N+M コールドスタンバイを構成する場合は，予備サーバブレードには N+M 切り替え時に HVM が起動できるように，あらかじめ以下の情報を設定してください。

  (1)動作モードの設定

  Web コンソールで動作モードを HVM に設定してください。

  (2)HVM ファームウェアの選択

  Web コンソールで HVM ファームウェアの割り当てを行ってください。

  (3)HVM の初期設定

  Web コンソールで以下の項目の設定を行ってください。

  - HVM IP アドレス
  - サブネットマスク
  - VNIC System No.
  - タイムゾーン

  動作モードの設定，HVM ファームウェアの選択，HVM の初期設定の詳細については「*BladeSymphony BS500 サーバブレードセットアップガイド*」を参照してください。
- OS およびアプリケーションでの稼働条件を満たしていること。
- Emulex 8Gb 2 ポートファイバチャネル拡張カードおよび Emulex 16Gb 2 ポートファイバチャネル拡張カードを用いて，N+M コールドスタンバイを構成する場合，HBA BIOS 設定のセットアップメニューの全項目を引き継ぎます。そのため，現用サーバブレードと LU 間の SAN 構成と予備サーバブレードと LU 間の SAN 構成が等価であること。
  - FC スイッチのカスケード段数
  - FC スイッチのポートスピード設定
  - ディスク装置のポートスピード設定やトポロジの設定
- Emulex 10Gb CNA/LAN 拡張カード，オンボード CNA(2 ポート/4 ポート)を用いて N+M コールドスタンバイを構成する場合，現用サーバブレードと予備サーバブレードに搭載される Emulex 10Gb CNA/LAN 拡張カード，オンボード CNA(2 ポート/4 ポート)の設定は必ず次の設定としてください。
  - MultiChannel Support 設定は，現用サーバブレードと予備サーバブレードで一致させること
  - Personality 設定は，現用サーバブレードと予備サーバブレードで一致させること
  - CNA/LAN 拡張カード，オンボード CNA(2 ポート)の場合，Personality 設定は，NIC または iSCSI とすること。オンボード CNA(4 ポート)の場合，Personality 設定は，NIC または NIC+RoCE とすること
  - iSCSI 設定の DHCP は Disable とすること
  - iSCSI Initiator IP Address は重複しないよう設定すること
  - iSCSI Target は正常に接続している状態(Connected)にすること
  - iSCSI Target のセッション数は 1 ポートあたり 4 セッションまでとすること

  MultiChannel Support 設定，Personality 設定の詳細については，「*OneCommanndManager ガイド*」を参照してください。

2.14.6 N+M コールドスタンバイ使用時の注意事項

- 現用系サーバブレードと予備サーバブレードに搭載される Emulex 10Gb CNA/LAN 拡張カード，オンボード CNA の設定が上記でない場合，N+M 切り替えは正常に動作しません。
- BS520H サーバブレード A1/B1，BS520A サーバブレード A1 の Emulex 10Gb CNA/LAN 拡張カードあるいはオンボード CNA(2 ポート)の NIC 設定を N+M コールドスタンバイで引継ぐには，次に示すファームウェアバージョンを使用してください。

  マネジメントモジュール

  A0125 以降

  サーバブレードファームウェア

  ・BS520H サーバブレード A1/B1 の場合は，統合ファームウェア 01-44 以降

  ・BS520A サーバブレード A1 の場合は，統合ファームウェア 02-16 以降

- BS520H サーバブレード A1/B1，BS520A サーバブレード A1 , BS540A サーバブレード A1/B1 の Emulex 10Gb CNA/LAN 拡張カードあるいはオンボード CNA(2 ポート)の iSCSI 設定を N+M コールドスタンバイで引継ぐには，次に示すファームウェアバージョンを使用してください。

  マネジメントモジュール

  A0135 以降

  サーバブレードファームウェア

  ・BS520H サーバブレード A1/B1 の場合は，統合ファームウェア 01-57 以降

  ・BS520A サーバブレード A1 の場合は，統合ファームウェア 02-28 以降

  ・BS540A サーバブレード A1/B1 の場合は，統合ファームウェア 03-09 以降

- また，Personality が iSCSI の場合は，誤接続を防ぐため，予備サーバブレードの iSCSI 設定を次のように設定する必要があります。

  iSCSI Initiator IP Address

  0.0.0.0

  iSCSI Initiator SubnetMask

  0.0.0.0

- Emulex 10Gb CNA/LAN 拡張カードあるいはオンボード CNA(2 ポート)の NIC 設定を N+M コールドスタンバイで引継ぐには，「表 2-84 ファームウェアバージョンとドライバの構成」に記載のファームウェアバージョンとドライバの構成を使用してください。

表 2-84 ファームウェアバージョンとドライバの構成

現用サーバブレードに搭載されている CNA ファームウェア	予備サーバブレードに搭載されている CNA ファームウェア	LAN ドライバ	
		Windows	Linux
4.1.334.28/4.1.334.2801	4.1.334.28/4.1.334.2801	4.1.334.25	4.1.334.18
4.2.433.604	4.1.334.28/4.1.334.2801	4.1.334.25	4.1.334.18
4.1.334.28/4.1.334.2801	4.2.433.604	4.1.334.25	4.1.334.18
4.2.433.604	4.2.433.604	4.2.390.6	4.2.456.0

※LAN ドライバが 4.2.390.6 または，4.2.456.0 構成で，CNA のファームウェアが 4.1.334.28 または，4.1.334.2801 の構成は，サポートしていません。

- Emulex 10Gb CNA(4 ポート)を有効とした N+M コールドスタンバイのサポート機能はファームウェアバージョンによって異なります。

次に示すファームウェアバージョンでは，現用サーバブレードの Emulex 10Gb オンボード CNA(4 ポート)に割り当てた additional MAC アドレスのみ，予備サーバブレードに引き継ぐことができます。このため，N+M コールドスタンバイを使用する場合は，オンボード CNA(4 ポート)の設定を必ず次の設定としてください。次の設定でない場合の N+M コールドスタンバイは非サポートのため，使用しないでください。

- オンボード CNA(4 ポート)の Personality 設定は NIC または NIC+RoCE であること
- オンボード CNA(4 ポート)の設定は現用サーバブレードと予備サーバブレードで一致させること

マネジメントモジュール

A0230 以降

サーバブレードファームウェア

BS520X サーバブレード B1：06-13 以降

BS520H サーバブレード B3：08-10～08-12

- 次に示すファームウェアバージョンでは，BS520X サーバブレード B1，BS520H サーバブレード B3 のオンボード CNA(4 ポート)の Personality 設定が NIC または NIC+RoCE の場合，現用サーバブレードのオンボード CNA(4 ポート)に割り当てた additional MAC アドレスおよびオンボード CNA(4 ポート)の設定情報を引き継ぐことができます。ただし，Personality 設定を iSCSI とした N+M コールドスタンバイは非サポートです。

  マネジメントモジュール

  A0240 以降

  サーバブレードファームウェア

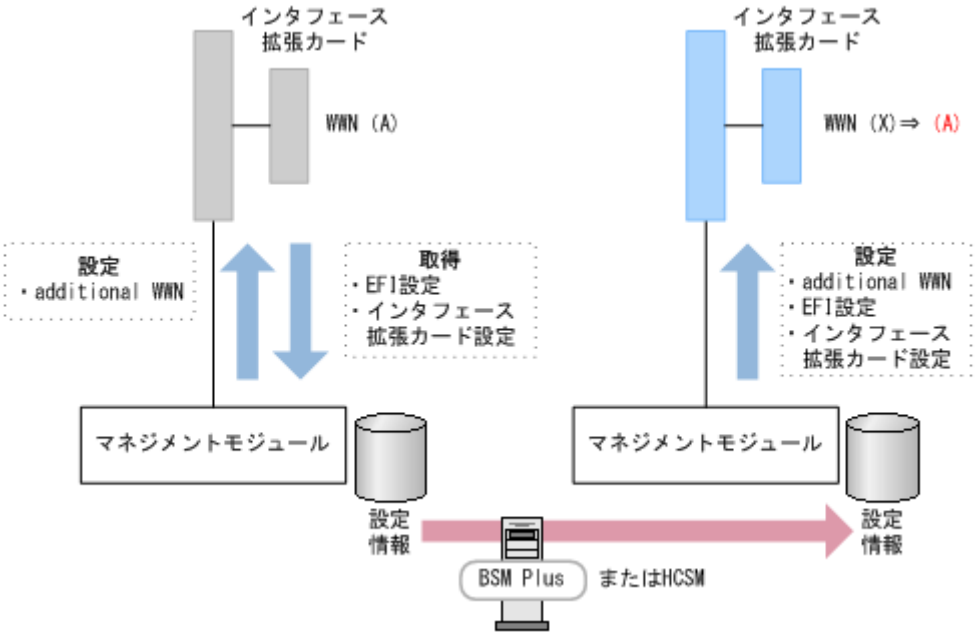
  BS520X サーバブレード B1：07-24 以降

  BS520H サーバブレード B3：08-16 以降

2.14.7 N+M コールドスタンバイにおける Pre-configure

N+M コールドスタンバイでは，現用サーバブレードの設定情報をあらかじめ取得し，マネジメントモジュールに保持しておきます。また，N+M 切り替え時にはマネジメントモジュールに保持しておいた設定情報を予備サーバブレードに設定し予備サーバブレードを起動します。

Pre-configure による現用サーバブレードの設定情報の取得は，N+M 切り替え時ではなく，N+M コールドスタンバイ構築時に実行されている必要があります。これは，障害発生サーバブレードでは Pre-configure を実行できない場合があるためです。



2.14.8 Pre-configure 実行契機

Pre-configure は，次の場合にサーバブレードに対して設定情報を取得，および設定するために手動，あるいは自動で実行されます。

- マネジメントモジュールのコンソールからの Pre-configure 実行時
- N+M 切り替えからの復帰時（BSM Plus または HCSM による実行）
- システム装置の電源投入時
- サーバブレード構成変更時

(1) マネジメントモジュールのコンソールからの Pre-configure 実行時

マネジメントモジュールのコンソールから次の操作を行うと Pre-configure を実行することができます。

Pre-configure 実行

この Pre-configure 実行は，サーバブレードの設定が完了し SAN ブートが可能になった後，サーバブレードの設定情報をマネジメントモジュールに保持するために実行します。

表 2-85 Web コンソールでの操作方法

項目	画面
Pre-configure 実行	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 状態タブ → サーバブレード操作 → Pre-configure 実行

N+M コールドスタンバイ支援機能の有効化設定

N+M コールドスタンバイ支援機能を無効から有効に設定変更した場合にも，ファイバチャネル拡張カードに additional WWN を設定するために Pre-configure が実行されます。

参考 SMP 構成の場合，プライマリサーバブレードに指定した設定内容で動作します。ノンプライマリサーバには設定しないでください。

表 2-86 Web コンソールでの操作方法

項目	画面
N+M コールドスタンバイ支援機能の有効化設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 設定タブ → サーバブレード設定

(2) N+M 切り替えからの復帰時（BSM Plus または HCSM による実行）

N+M 切り替え済みの状態から，元の状態にサーバブレードを復帰する場合，現用サーバブレードに関しては同様に Pre-configure は実行しませんが，予備サーバブレードに関しては，切り替え可能な状態とするため，Pre-configure が実行されます。

本契機での Pre-configure は BSM Plus または HCSM により自動で実行されます。

(3) システム装置の電源投入時

N+M コールドスタンバイを構築した後，システム装置の電源を遮断，投入した場合，自動的に Pre-configure が実行され，N+M コールドスタンバイが復帰します。

(4) サーバブレード構成変更時

次に示すサーバブレードの構成を変更した場合，マネジメントモジュールにより Pre-configure が自動実行され，マネジメントモジュール内の設定情報を更新します。

- サーバシャーシにサーバブレードを挿入した時
- サーバブレードに電源を投入した時

2.14.9 Pre-configure 実行中のサーバブレードの動作

Pre-configure 実行中は，サーバブレード前面の識別 LED が点滅します。また，識別 LED が点滅している間，サーバブレードには一時的に電源が投入されます。点滅する識別 LED の詳細は「*BladeSymphony BS500 システム概要*」を参照してください。

2.14.10 Pre-configure 実行所要時間

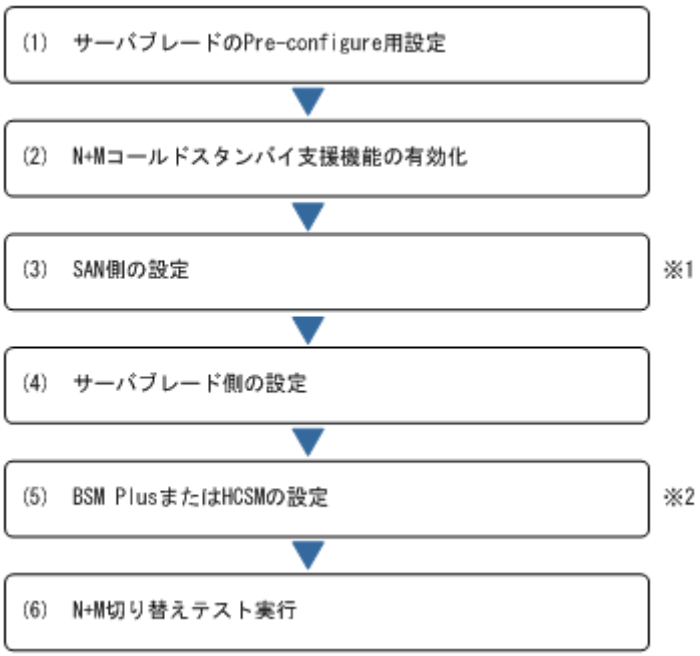
Pre-configure 実行の所要時間は３～１５分です。

所要時間は，サーバブレード種，搭載 CPU 数，メモリ，PCI カード種および搭載数などにより異なります。

2.14.11 N+M コールドスタンバイ構築手順

N+M コールドスタンバイの設定には BladeSymphony, SAN および BSM Plus または HCSM のそれぞれで設定が必要です。SAN および BSM Plus または HCSM の設定は個々の取扱説明書，マニュアルを参照してください。

N+M コールドスタンバイ構築の設定の大まかな流れを説明します。個々の手順は以降の節で説明します。



※1：詳細は該当製品の取り扱い説明書を参照してください。

※2：詳細は BSM Plus または HCSM のマニュアル，ヘルプなどを参照してください。

(1) サーバブレードの Pre-configure 用設定

N+M コールドスタンバイを構築する場合，サーバブレードで次の設定をしておく必要があります。

- 内蔵 HDD を無効にする

  N+M コールドスタンバイでは内蔵 HDD を使用できません。内蔵 HDD が搭載されている場合は UEFI 設定で無効にしておく必要があります。

重要 UEFI セットアップメニューで EFI Shell のブート優先順位を最上位に変更しないでください。EFI Shell のブート優先順位が最上位の場合，N+M 切り替え，復帰を実行しても正常に OS が起動しません。

(2) N+M コールドスタンバイ支援機能の有効化

現用サーバブレード，予備サーバブレードの両方で N+M コールドスタンバイ支援機能を有効（Enable）にします。このとき，N+M コールドスタンバイ支援機能が有効にしたサーバブレードに対して，直ちに Pre-configure が実行されます。この Pre-configure によりファイバチャネル拡張カードに additional WWN を設定します。

表 2-87 Web コンソールでの操作方法

項目	画面
N+M コールドスタンバイ支援機能の有効化設定	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 設定タブ → サーバブレード設定

また，ウォッチドッグタイムアウトを契機に N+M 切り替えを実行したい場合，WDT タイムアウト N+M 切替設定を有効（Enable）にします。システム装置の工場出荷時には無効（Disable）に設定されています。

表 2-88 Web コンソールでの操作方法

項目	画面
WDT タイムアウト N+M 切替設定	Resources タブ → Modules → 全モジュール → シャーシ → 設定タブ

参考

- Pre-configure 実行には「2.14.10 Pre-configure 実行所要時間」に示す時間がかかります。
- HVM モードで N+M コールドスタンバイを構築する場合でも，前述の「(1) サーバブレードの Pre-configure 用設定」，「(2) N+M コールドスタンバイ支援機能の有効化」の手順を実施する必要があります。
- SMP 構成の場合，プライマリサーバブレードに指定した設定内容で動作します。ノンプライマリサーバには設定しないでください。

(3) SAN 側の設定

Basic モードのサーバブレードの場合

ファイバチャネル接続の場合，SAN で WWN などを設定します。WWN には additional WWN を使用してください。additional WWN の確認方法は，「2.10.7 WWN，MAC アドレスの確認方法」を参照してください。iSCSI 接続の場合，SAN で iSCSI Target などを設定します。

HVM モードのサーバブレードの場合

SAN で WWN などを設定します。WWN には virtual FC WWN を使用してください。virtual FC WWN については「*BladeSymphony BS500 HVM ユーザーズガイド*」を確認してください。

参考 本設定は FC スイッチ，SAN，LUN Manager などでの設定です。詳細は当該製品の取扱説明書を参照してください。

(4) サーバブレード側の設定

Basic モードのサーバブレードの場合

現用サーバブレードが SAN からブートできるように設定します。

- ファイバチャネル拡張カードの設定
  - ファイバチャネル拡張カード BIOS を Enable，ブートプライオリティを Enable に設定します。
  - ブート対象 LU を選択します。

  詳細な設定方法は，ファイバチャネル拡張カードのマニュアルを参照してください。
- CNA(iSCSI)の設定
  - iSCSI Target などを設定します。

  詳細な設定方法は，「*BladeSymphony BS500 EFI ユーザーズガイド*」を参照してください。
- UEFI 設定
  - ブート優先順位を設定し，SAN からブート可能に設定にします。

  詳細な設定方法は，「*BladeSymphony BS500 EFI ユーザーズガイド*」を参照してください。

HVM モードのサーバブレードの場合

現用サーバブレード上の HVM で稼働する LPAR が SAN からブートできるように設定します。

- UEFI 設定
  - HVM が起動するために必要な UEFI 設定であることを確認します。

  詳細については「*BladeSymphony BS500 サーバブレードセットアップガイド*」を参照してください。
- Pre-State Auto Activate の設定

- N+M 切り替え後，LPAR を自動 Activate させるために，HVM スクリーンより Pre-State Auto Activation を Yes に設定します。

詳細については「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

- LPAR 構成
  - LPAR に必要なプロセッサ，メモリ，占有 PCI デバイス，共有デバイス（VNIC，共有 FC）を割り当てます。
  - 当該 LPAR を Activate にします。

詳細については「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

- ファイバチャネル拡張カードのデバイス設定（占有または共有）
  - LPAR の UEFI メニューから EFI Shell を選択し，Shell プロンプトから drvcfg コマンドを用いて，デバイス設定シェル(hfccfg)を呼び出します。
  - ブート対象 LU が接続されている HBA FC Port の Boot Function を Enable に設定します。

詳細な設定方法は，ファイバチャネル拡張カードのマニュアルを参照してください。

- ブート設定
  - LPAR の UEFI メニューから Boot option maintenance menu メニューを選択し，ブートパス，ブートオーダを設定し，SAN からブート可能に設定にします。

詳細については「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

重要 LPAR の構成（プロセッサ，メモリ，デバイス割り当て）を変更した場合は，必ず HVMMenu スクリーンで[F9]:Save Configuration を実行してください。詳細については「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

(5) BSM Plus または HCSM の設定

BSM Plus または HCSM で N+M コールドスタンバイを設定（現用サーバブレード，予備サーバブレードの決定など）します。（本設定は BSM Plus または HCSM での設定です。詳細は BSM Plus または HCSM のマニュアルを参照してください）

なお，設定に際し，次の事前確認を実施してください。

- N+M コールドスタンバイ支援機能が有効に設定されていること。

  現用サーバブレード, 予備サーバブレードの両方で有効となっている必要があります。確認方法については「(2) N+M コールドスタンバイ支援機能の有効化」を参照してください。
- Basic モードの場合，現用サーバブレードが SAN からブートすること。
- HVM モードの場合，現用サーバブレード上の HVM に構成した LPAR が SAN からブートすること。

事前確認が完了後，BSM Plus または HCSM を使用し，N+M コールドスタンバイを設定してください。

重要 LPAR の構成（プロセッサ，メモリ，デバイス割り当て）を変更した場合は，必ず HVM Menu スクリーンで[F9]:Save Configuration を実行してください。詳細については「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

(6) N+M 切り替えテスト実行

運用を開始する前に，BSM Plus からの「手動切り替え実行」，もしくは HCSM からの「N+M コールドスタンバイテスト」の実行，もしくはマネジメントモジュールのコンソールからの切り替えテストアラート発行により，N+M 切り替えテストを実施し，正常に N+M 切り替えができることを確認してください。

表 2-89 Web コンソールでの操作方法

項目	画面
(BSM Plus から)N+M コールドスタンバイにおける現用系サーバブレードの切り替えテストのためのアラートを発行する	Administration タブ → JP1/SC/BSM 連携 → Action → アラート送信
(HCSM から)N+M コールドスタンバイにおける現用系サーバブレードの切り替えテストのためのアラートを発行する	Administration タブ → HCSM 連携 → Action → アラート送信

重要

- 切り替えアラートを発行した場合，現用サーバブレードの電源が強制 OFF されます。
- SMP 構成の場合，プライマリサーバブレードに対して切り替えアラートを発行します。ノンプライマリサーバブレードに対して切り替えアラートを発行すると，切替テストに失敗します。

参考 N+M コールドスタンバイ構築および N+M 切り替え手順の詳細は，BSM Plus または HCSM のマニュアルを参照してください。

2.14.12 N+M コールドスタンバイ構築後の設定変更

(1) Basic モードのサーバブレードの場合

N+M コールドスタンバイ構築後に，マネジメントモジュールの Web コンソールから UEFI 設定を変更した場合，UEFI 設定は次回の UEFI 起動時に適用されます。UEFI 設定を変更した後，その UEFI 設定が適用されるまでの間に N+M 切り替えが発生した場合は，前回の UEFI 起動時の設定で引継ぎが実行されます。

(2) HVM モードのサーバブレードの場合

N+M コールドスタンバイ構築後に，LPAR の構成（プロセッサ，メモリ，デバイス割り当て）を変更した場合は，必ず HVM Menu スクリーンで[F9]:Save Configuration を実行してください。Save Configuration を実行しない場合，実際の HVM 構成情報とマネジメントモジュールが保持する HVM 構成情報に差異が発生するため，N+M 切り替えに失敗する可能性があります。

2.14.13 N+M コールドスタンバイ構築後の CNA 交換

CNA を Personality:iSCSI の設定で使用している構成で，CNA 交換後の iSCSI 設定の復旧作業が必要となった場合，N+M コールドスタンバイの状態により次のような設定を行う必要があります。

状態	設定内容
N+M で切り替わっていない状態での現用系	交換前の現用系の iSCSI 設定に戻す。
N+M で切り替わっていない状態での予備系	交換前の予備系の iSCSI 設定に戻す。 (iSCSI 接続が切断されている状態の設定)
N+M で切り替わっている状態での現用系	交換前の予備系の iSCSI 設定に戻す。 (iSCSI 接続が切断されている状態の設定)
N+M で切り替わっている状態での予備系	交換前の現用系の iSCSI 設定に戻す。

2.14.14 N+M コールドスタンバイの UPS 接続設定

USP 接続時，電源復旧後に自動的に N+M コールドスタンバイを復元する場合，サーバブレードの電源自動投入の設定が必要です。次の手順を実施してください。

1. 電源復旧後に自動的に現用サーバブレードに電源を投入する設定にします。

表 2-90 Web コンソールでの操作方法

項目	画面
サーバブレードの AC recovery を「Power ON」に設定する	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 設定タブ → サーバブレード設定

この設定では，電源復旧後に電源が投入されます。

2. 予備サーバブレードの自動電源投入を抑止します。

表 2-91 Web コンソールでの操作方法

項目	画面
サーバブレードの AC recovery を「Power OFF」に設定する	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → 設定タブ → サーバブレード設定

これにより，電源復旧時の電源自動投入が抑止されます。

参考

- UPS 接続時でも，電源復旧後にサーバブレードの自動起動を必要としない場合，本設定は不要です。
- 「(2) N+M コールドスタンバイ支援機能の有効化」で N+M コールドスタンバイ支援機能を有効(enable)設定している場合，UEFI セットアップメニューで電源供給復帰時のサーバの自動電源投入を有効にしても，サーバブレードの AC recovery 設定が「Power ON」に設定されていない場合には，電源供給復旧時にサーバブレードが自動起動しない場合があります。
- SMP 構成の場合，プライマリサーバブレードの設定が SMP を構成するすべてのサーバブレードに適用されます。ノンプライマリサーバブレードの設定は不要です。

2.15 HA モニタ連携

マネジメントモジュールと HA モニタの連携について説明します。

2.15.1 HA モニタ概要

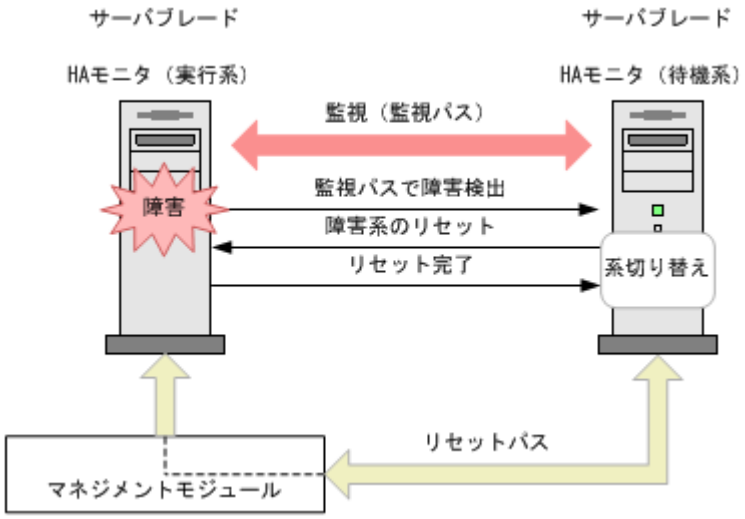
HA モニタは，システムの信頼性向上，稼働率向上を目的として，プログラムを含めたシステムの切り替えを実現します。

HA モニタを使用すると，業務処理を実行中のサーバブレード(実行系)に障害が発生した場合，事前に待機しているサーバブレード(待機系)に，直ちに自動で切り替えることができます。そのため，オペレータが特に意識することなく，システムの信頼性や稼働率を高められます。

この実行系と待機系により構成されるホットスタンバイ構成を系切り替え構成と呼びます。

参考 HA モニタの詳細については，「高信頼化システム監視機能 HA モニタ」(3000-9-132)を参照してください。

マネジメントモジュールは，系障害が発生した場合の系切り替えを支援するために，HA モニタから要求される系のリセットを行います。また，障害が発生したときに，確実に系がリセットできるように，リセットの経路(リセットパス)を監視しています。



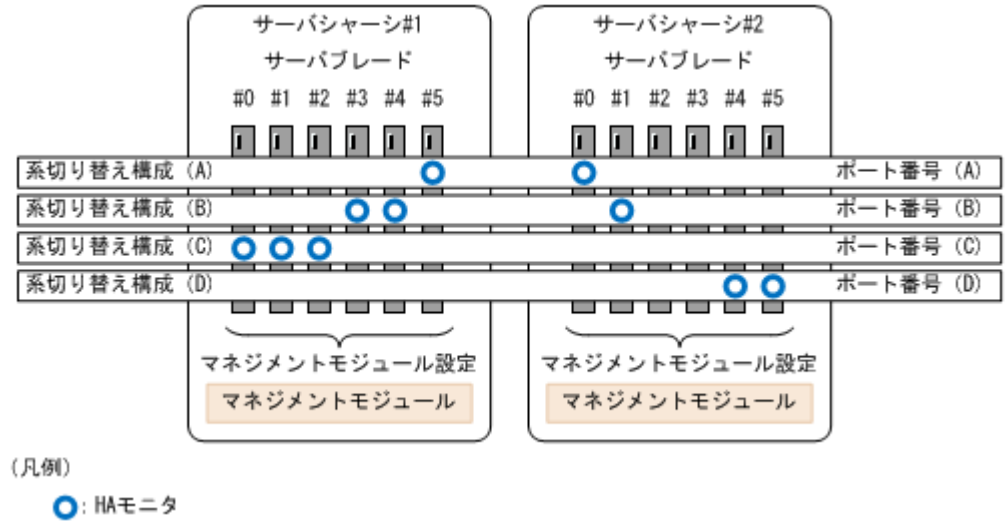
2.15.2 系切り替え構成の設定方法

HA モニタの系は，サーバブレードごとに割り当てます。それぞれの系切り替え構成が，互いに干渉しないように，系切り替え構成で使用するポート番号は，それぞれ別のポート番号を割り当てるようにしてください。各設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。

表 2-92 Web コンソールでの操作方法

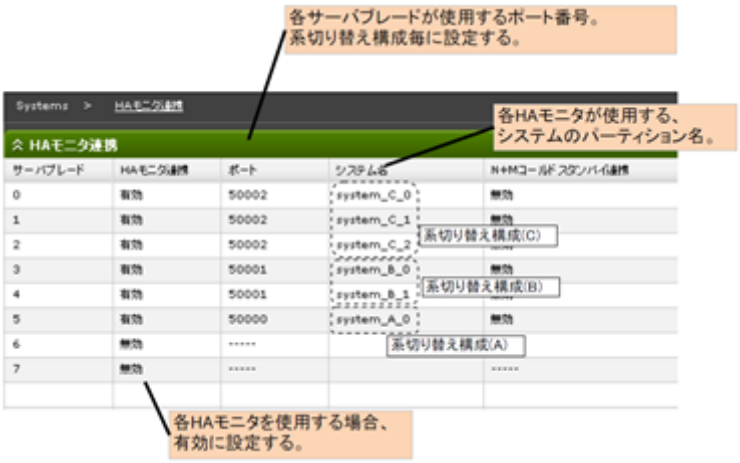
項目	画面
HA モニタの表示，設定	Resources タブ → Systems → HA モニタ連携 → 該当サーバブレードをクリック → 設定

次に系切り替え構成の設定例を示します。

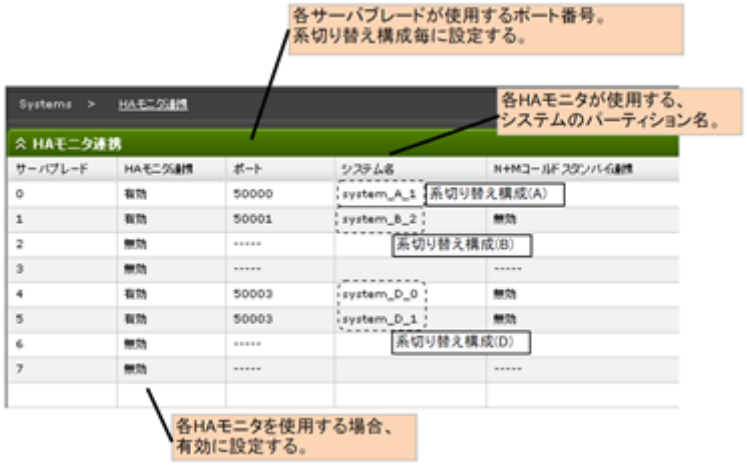


サーバシャーシ#1 とサーバシャーシ#2 のような系切り替え構成を Web コンソールにより設定する場合，次のように設定します。

- マネジメントモジュール(サーバシャーシ#1)設定例



- マネジメントモジュール(サーバシャーシ#2)設定例

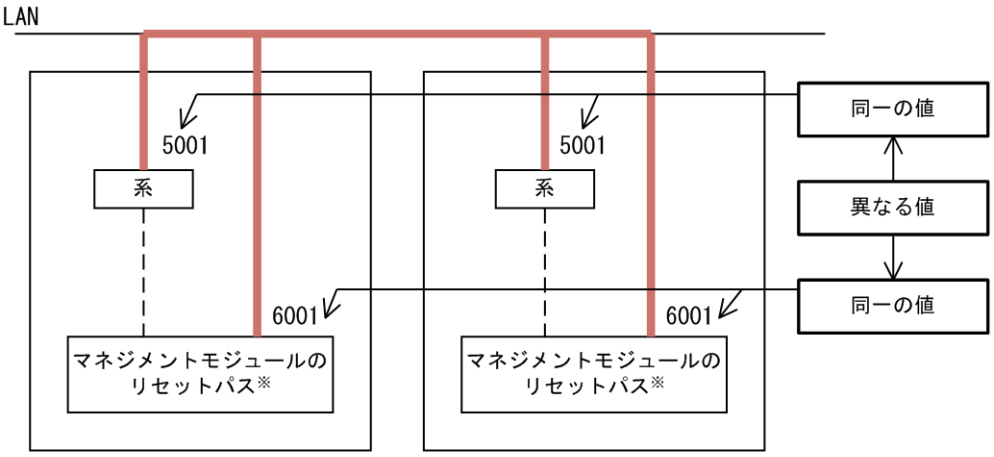


重要 HVM モードのサーバブレードで稼働する LPAR について，LPAR 番号 31 以降の LPAR を HA モニタによる系切り替え対象とする場合は，マネジメントモジュールファームウェアバージョン A0235 以降を適用してください。

リセットパスのポート番号を決める際の注意事項

1. 同一 LAN 上にある HA モニタの系とマネジメントモジュールは，ポート番号が同一の値である系と，ポート番号が同一の値であるマネジメントモジュールで，リセットパスの通信を行います。マネジメントモジュールのポート番号は，系のポート番号とは異なる値にしてください。

図 2-3 リセットパスの構成例 1



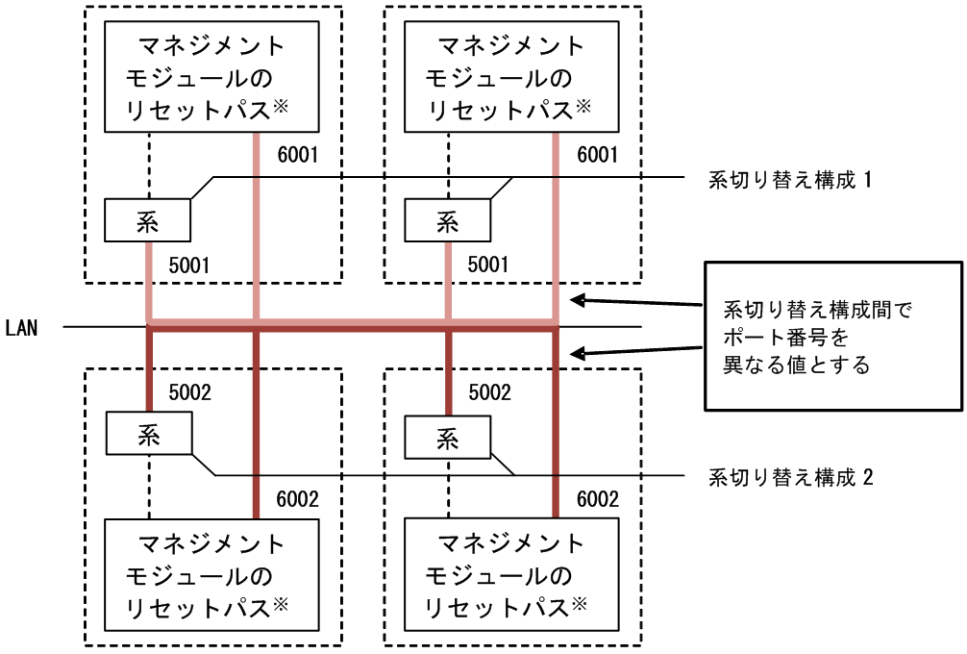
注※
サーバブレード単位に設定可能

2. 同一の LAN 上に複数の系切り替え構成を構築する場合は，下記のどちらかの設定としてください。また，HA モニタのマニュアルのリセットパスの構成の注意事項も参照してください。

ケース 1

系切り替え構成間で，系のポート番号を異なる値とし，マネジメントモジュールのポート番号も異なる値としてください。図 2-4 に定義例を示します。

図 2-4 リセットパスの構成例 2

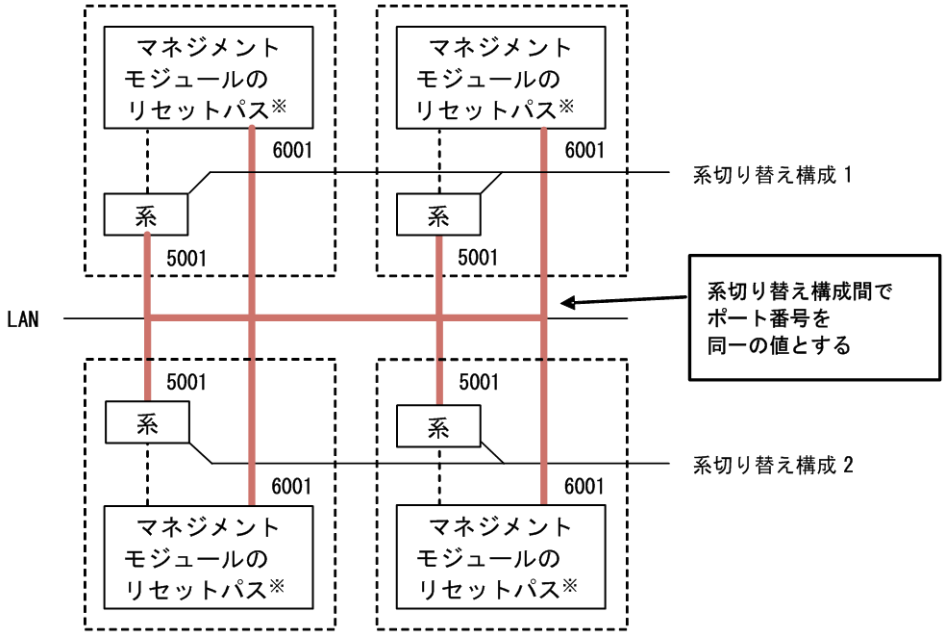


注※
サーバブレード単位に設定可能

ケース 2

系切り替え構成間で，系のポート番号を同一の値とし，マネジメントモジュールのポート番号も同一の値としてください。図 2-5 に定義例を示します。

図 2-5 リセットパスの構成例 3



注※
サーバブレード単位に設定可能

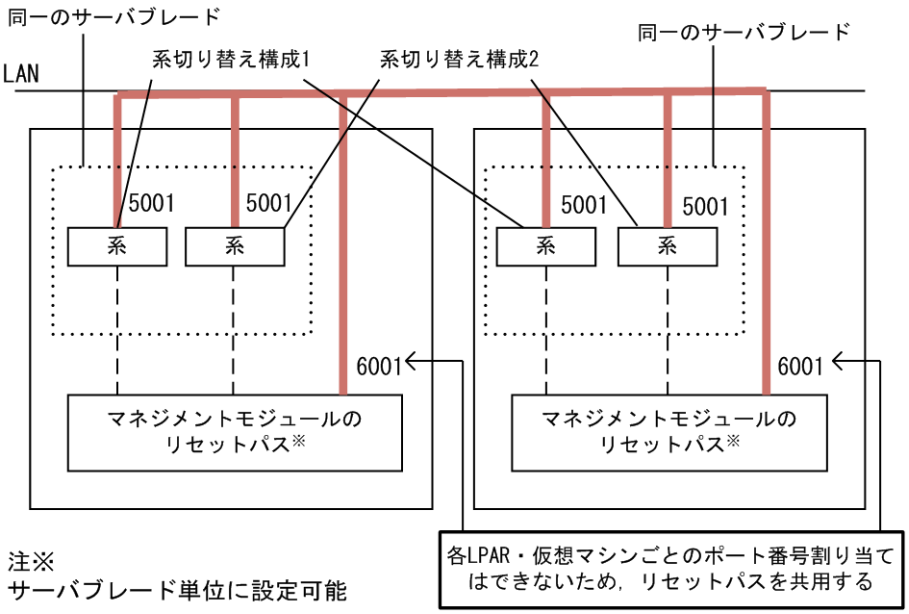
ケース 2 は系切り替え構成間でリセットパスの通信が干渉することになるため，ケース 1 を推奨します。

重要 次のような系切り替え構成は設定しないでください。系切り替えに失敗することがあります。

- 系切り替え構成間で，系のポート番号を異なる値とし，マネジメントモジュールのポート番号を同一の値としている。
- 系切り替え構成間で，系のポート番号を同一の値とし，マネジメントモジュールのポート番号を異なる値としている。

3. 仮想化環境で，LPAR または仮想マシンを系とした系切り替え構成の場合，同一のサーバブレード上の系は，マネジメントモジュールのリセットパスを共用する構成となります。系のリセットパスのポート番号とマネジメントモジュールのポート番号の設定は同一の値としてください。

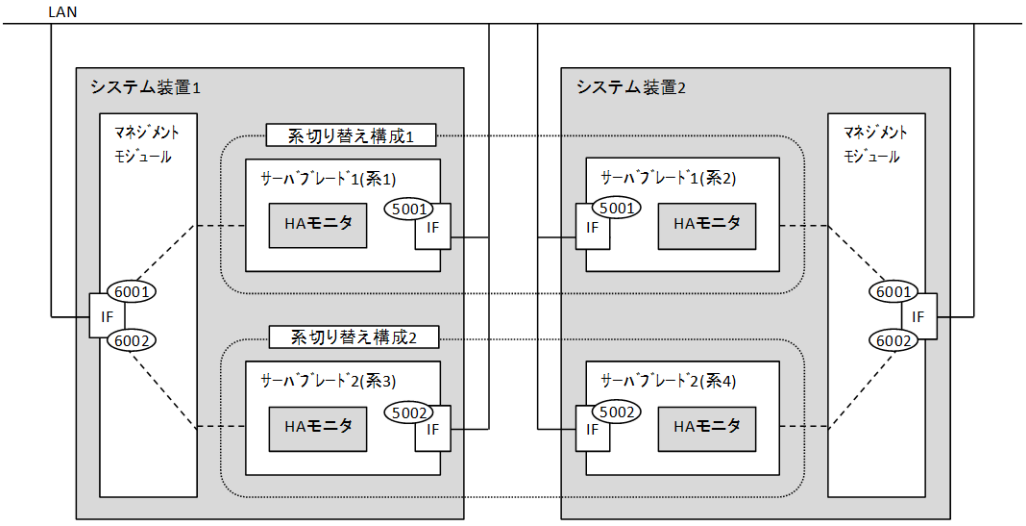
図 2-6 リセットパスの構成例 4



リセットパスのポート番号の具体的な設定例

2 台のシステム装置の各 2 台のサーバブレードで，系切り替え構成を 2 つ構築する場合を例に，具体的な設定例を示します。

図 2-7 リセットパスのポート番号の具体的な設定例



- 各系切り替え構成は，リセットパスに以下のポート番号を用います。

表 2-93 系切り替え構成のリセットパスのポート番号

ポート	系切り替え構成 1	系切り替え構成 2
系のリセットパスのポート番号	5001	5002
マネジメントモジュールのポート番号	6001	6002

- システム装置 1 のマネジメントモジュールには次のように設定してください。
  HA モニタ連携のサーバブレード 1（系 1）のポート番号：6001
  HA モニタ連携のサーバブレード 2（系 3）のポート番号：6002

- システム装置２のマネジメントモジュールには次のように設定してください。
  HA モニタ連携のサーバブレード１（系２）のポート番号：6001
  HA モニタ連携のサーバブレード２（系４）のポート番号：6002
- 系１と系２の HA モニタには次のように設定してください。
  リセットパスのポート番号：5001
  SVP のポート番号：6001
- 系３と系４の HA モニタには次のように設定してください。
  リセットパスのポート番号：5002
  SVP のポート番号：6002

2.16 LDAP 連携

マネジメントモジュールと LDAP の連携について説明します。

2.16.1 概要

本システム装置では，Lightweight Directory Access Protocol（以降 LDAP）を用いて，LDAP サーバ上の LDAP ディレクトリを検索し，ユーザ認証を行うことができます。これにより次のことを実現することができます。

- LDAP ディレクトリ登録ユーザでのログイン
- LDAP ディレクトリの特定のグループに属するアカウントのみにログイン許可を与えるグループ認証

LDAP 連携をサポートしているモジュールは次のとおりです。

- マネジメントモジュール

LDAP 連携を行う場合，ユーザ認証時に，登録されたユーザアカウント情報または LDAP ディレクトリ上のユーザアカウント情報を元に，ログイン可否を判断します。LDAP サーバ上の LDAP ディレクトリにユーザアカウント情報を追加することで，LDAP サーバを利用するすべてのモジュールで追加されたユーザアカウント情報が利用可能となり，個々のモジュールにユーザアカウント情報を登録する必要がなくなります。

また，グループ認証を行うと，ユーザ認証時に LDAP ディレクトリ上のグループ情報を参照し，グループに所属するユーザアカウントのみログインを許可します。グループ認証を用いることで，すでに構築済みの LDAP ディレクトリに大きな変更を加えることなく，LDAP サーバ連携環境を構築することができます。

LDAP 連携を行わない場合は，個々のモジュールに登録されたアカウントでログイン可能です。

LDAP 連携を行う場合は，次の 2 つの認証方式を選択できます。

- 個々のモジュールに登録されたアカウントでのユーザ認証を先に実施し，認証失敗した場合は LDAP ディレクトリ上のアカウントでのユーザ認証を実施する方式
- LDAP ディレクトリ上のアカウントでのみユーザ認証を実施する方式

LDAP 連携を行う場合でも，前者の認証方式ならば個々のモジュールに登録されたアカウントでログインできます。

LDAP ディレクトリと各モジュールに同一名称のアカウントを登録した場合，前者の認証方式ならば個々のモジュールに登録されたアカウントで認証をまず行います。もし，個々のモジュールに登

録されたアカウントでの認証が失敗したときは LDAP ディレクトリ上のアカウントで認証を行います。

LDAP サーバは，最大 3 台登録することができます。複数登録した場合は，ユーザ認証実行時に，登録順に LDAP サーバへ接続を試みます。最初に接続に成功した LDAP サーバの LDAP ディレクトリを検索し，ユーザ認証を試みます。登録したすべての LDAP サーバへの接続に失敗した場合は，LDAP サーバを用いたユーザ認証は失敗します。

2.16.2 サポートする LDAP サーバ

本システム装置では，次に示す Windows Server に付属する Active Directory との連携をサポートします。

- Microsoft® Windows Server® 2008 R2, Standard
- Microsoft® Windows Server® 2008 R2, Enterprise
- Microsoft® Windows Server® 2008, Standard
- Microsoft® Windows Server® 2008, Enterprise
- Microsoft® Windows Server® 2012, Standard
- Microsoft® Windows Server® 2012, Datacenter

2.16.3 Active Directory の設定(Windows 側の設定)

Active Directory を LDAP サーバとして利用する際に必要な設定について説明します。

必要な設定項目を次の表に示します。

表 2-94 Active Directory の設定項目

#	設定項目
1	サーバ証明書
2	LDAP サーバへのバインド DN
3	マネジメントモジュールへのログイン用ユーザアカウント
4	マネジメントモジュールへのログインを許可するグループ

(1) サーバ証明書

システム装置と LDAP サーバとの通信は Secure Socket Layer（SSL）もしくは Transport Layer Security（TLS）を介して行うため，LDAP サーバとして使用する Active Directory にサーバ証明書の登録が必要です。サーバ証明書の登録手順については，ご使用の Windows Server のドキュメントを参照してください。

参考 サーバ証明書には，自己署名証明書，外部認証局により証明された証明書の二つがありますが，どちらをご使用いただいてもシステム装置と Active Directory の通信に影響はありません。

(2) LDAP サーバへのバインド DN

ユーザ認証時に LDAP ディレクトリを検索するためには，LDAP サーバに接続する必要があります。LDAP サーバに接続する方法には次の二つの方式があり，どちらか一方の設定を行ってください。

- LDAP バインド DN とパスワードを使用して接続する
- 無名（Anonymous）ユーザを使用して接続する

参考 LDAP バインド DN とパスワードを使用することを推奨します。

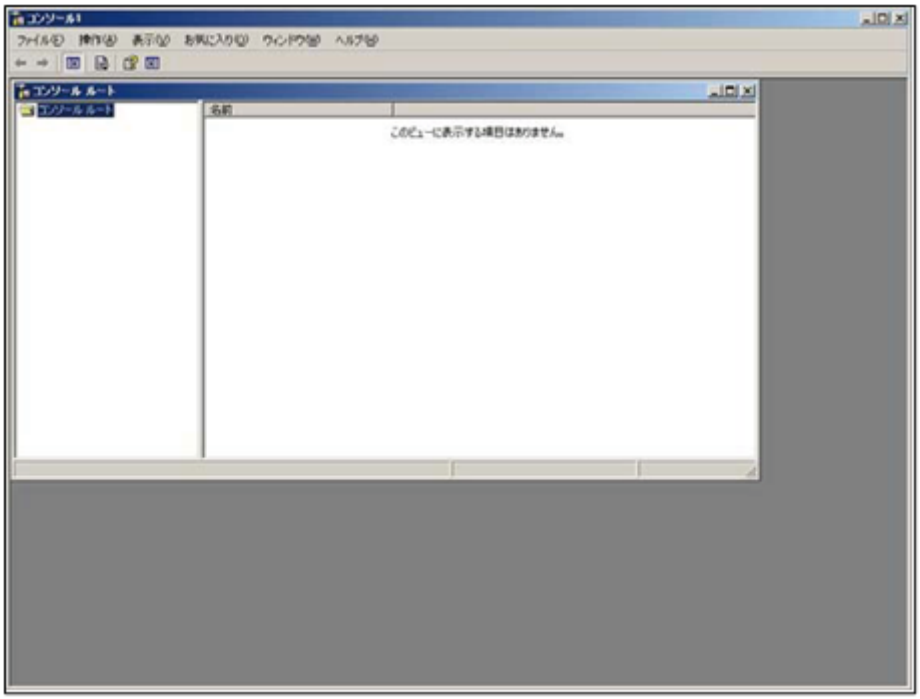
バインド DN として利用するユーザアカウントの登録

LDAP バインド DN として利用するユーザアカウントを，ご使用の Windows Server に登録します。ユーザの登録方法については，ご使用の Windows Server のドキュメントを参照してください。LDAP バインド DN として利用するユーザアカウントには，ユーザ認証に使用する LDAP ディレクトリに対するアクセス許可を付与する必要があります。

Anonymous ユーザの登録

Anonymous ユーザを登録する設定手順は次のとおりです。

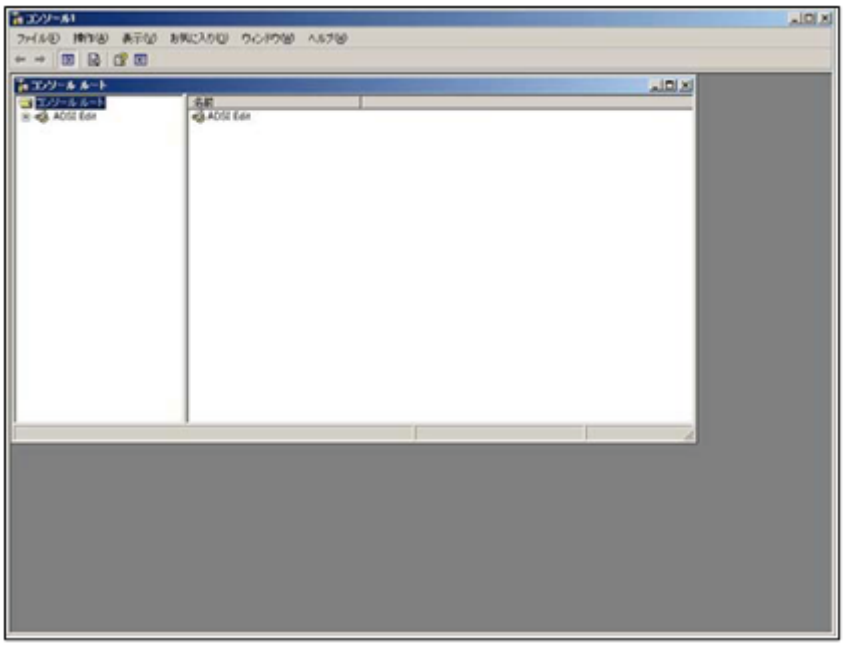
1. ［スタート > ファイル名を指定して実行］を選び，"mmc"を入力して［OK］ボタンをクリックしてください。



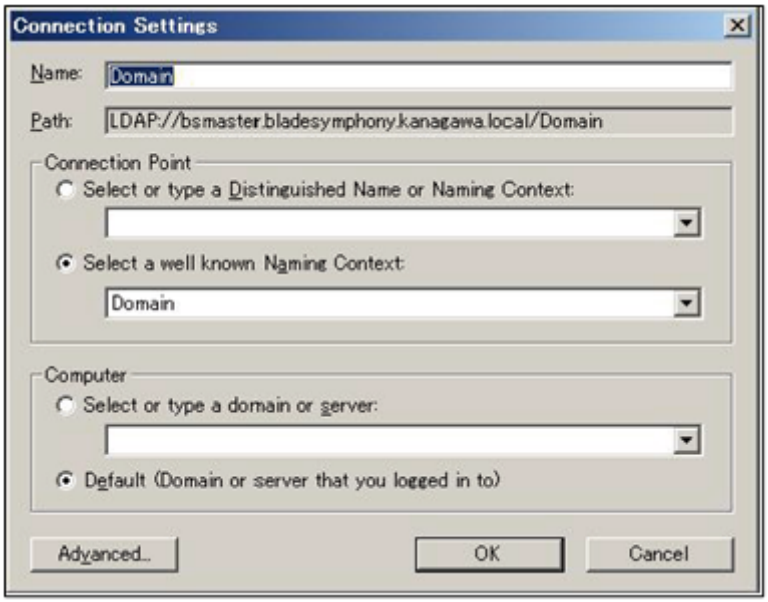
2. Microsoft Management Console（MMC）の画面が表示されたら，［メニュー > ファイル > スナップインの追加と削除］を選び，スナップインの追加画面から，［追加］ボタンをクリックしてください。

3. 追加できるスナップインの一覧から"ADSI Edit"を選択し，［追加］ボタンをクリックし，［閉じる］ボタンをクリックしてください。

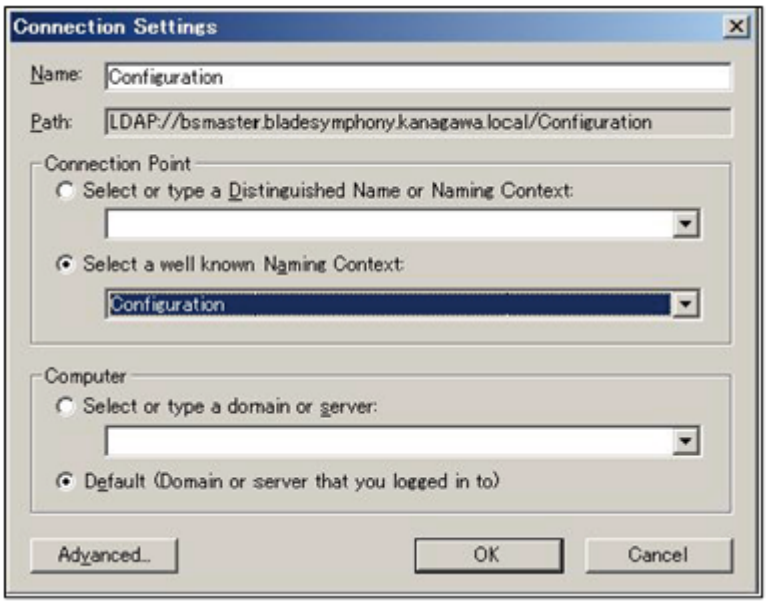
4. スナップインの追加と削除画面に"ADSI Edit"が追加されたら，［OK］ボタンをクリックしてください。



5. MMC 画面の［ADSI Edit］にマウスを合わせて右クリックし，"Connect to ..."を選択します。
6. 接続する Active Directory のドメインのコンテキストが選べるので，［Domain］を選び［OK］ボタンをクリックしてください。



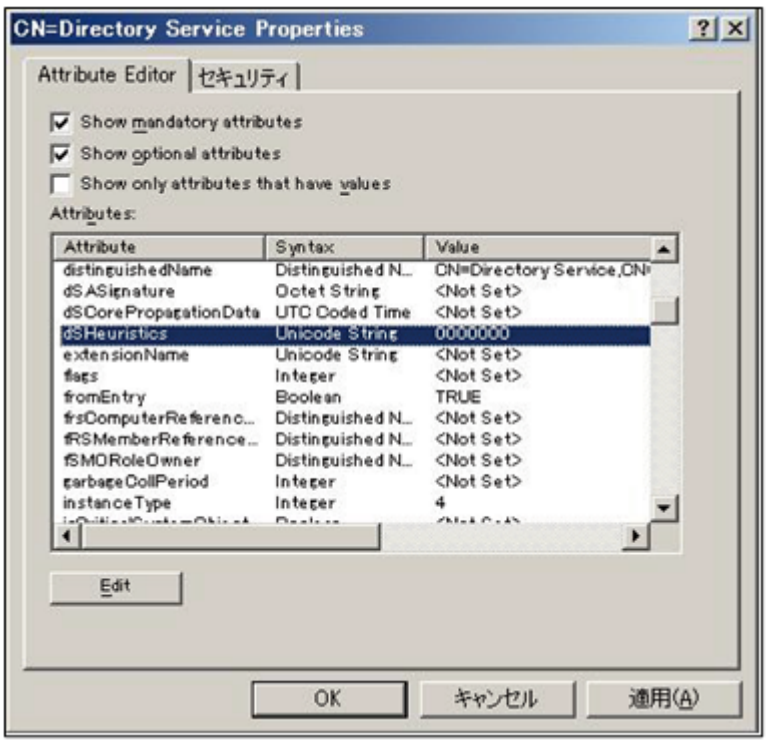
7. 再度［ADSI Edit］を右クリックし"Connect to ..."を選択します。
8. 今度はコンテキストとして，"Configuration"を選択し［OK］ボタンをクリックしてください。

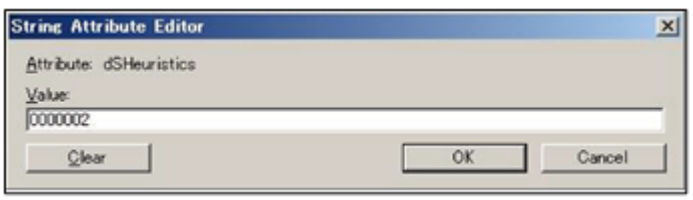


9. コントロールの［¥ADSI Edit¥configuration¥CN=Configuration¥DC= ドメインベース ¥CN=Services¥CN=Windows NT¥CN=Directory Service］にマウスを合わせて，右クリックして［プロパティ］を選択します。

10. プロパティ画面から"dSHeuristics"をクリックしてから［Edit］ボタンをクリックし，編集画面で値を設定します。

    本項目が設定されていない（<Not Set>の）場合は，"0000002"を設定します。既に何らかの値が設定されている場合には左から 7 番目だけを"2"にしてほかの値は変更しないでください。





11. 設定終了後，内容を反映させるためプロパティ画面で［OK］ボタンをクリックしてください。

以上で，Anonymous ユーザの登録が可能になります。

続いて，［管理ツール > Active Directory ユーザーとコンピュータ］から LDAP ディレクトリに対して Anonymous ユーザにアクセス権を付与します。

(3) マネジメントモジュールログイン用ユーザアカウントの登録

［管理ツール > Active Directory ユーザーとコンピュータ］から LDAP ディレクトリに対してユーザアカウントを登録します。登録の方法については，Windows Server のドキュメントを参照してください。ここでは，登録するユーザ名およびパスワードの制限，およびマネジメントモジュールログイン後に使用するロール情報の付与について説明します。

ユーザ名

ユーザ名として使用できる文字および文字長は，次のとおりです。

表 2-95 ユーザ名として使用できる文字および文字長

項目	説明
文字長	1-32 文字
使用可能文字（先頭）	[A-Z] [a-z]
使用可能文字（二文字目以降）	[A-Z] [a-z] [0-9]，"-"（ハイフン），"_"（アンダースコア），"."（ピリオド）

パスワード

パスワードとして使用できる文字および文字長は，次のとおりです。

表 2-96 パスワードとして使用できる文字および文字長

項目	説明
文字長	1-32 文字
使用可能文字	ASCII コード中の表示可能文字（0x20-0x7e）

参考 パスワードの複雑さについては，ご使用の Windows Server のセキュリティポリシーに依存します。

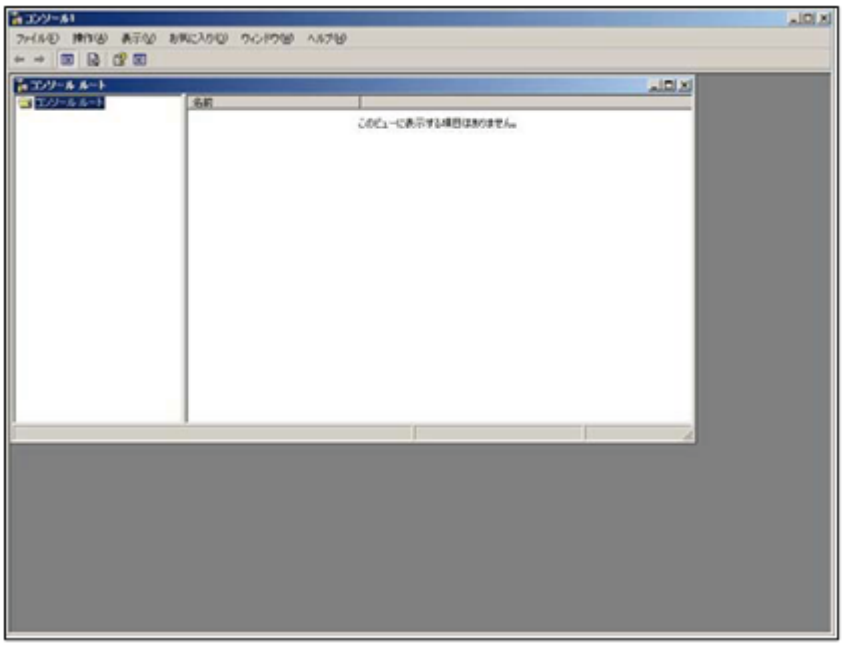
ロール情報付与

LDAP ディレクトリに登録したユーザアカウントに対して，ロール情報を付与することで，ログイン後に実行できる操作範囲を設定することができます。

参考 ロール情報を付与しない場合は，ログイン後に実行できる操作は最低限のものになります。

ロール情報を付与する手順は次のとおりです。

1. ［スタート > ファイル名を指定して実行］を選び，"mmc"を入力して［OK］ボタンをクリックしてください。

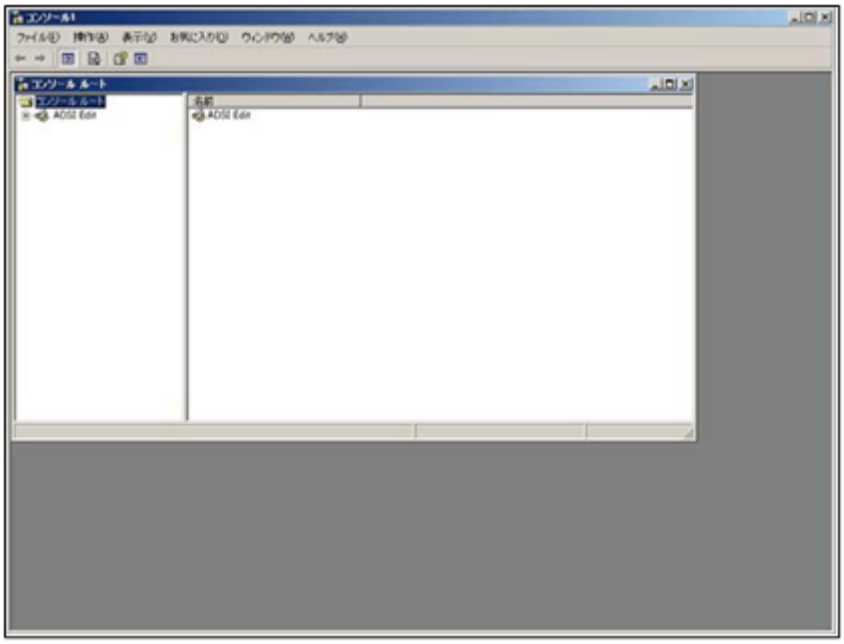


2. Microsoft Management Console（MMC）の画面が表示されたら，［メニュー > ファイル > スナップインの追加と削除］を選び，スナップインの追加画面から，［追加］ボタンをクリックしてください。

3. 追加できるスナップインの一覧から"ADSI Edit"を選択し，［追加］ボタンをクリックし，［閉じる］ボタンをクリックしてください。

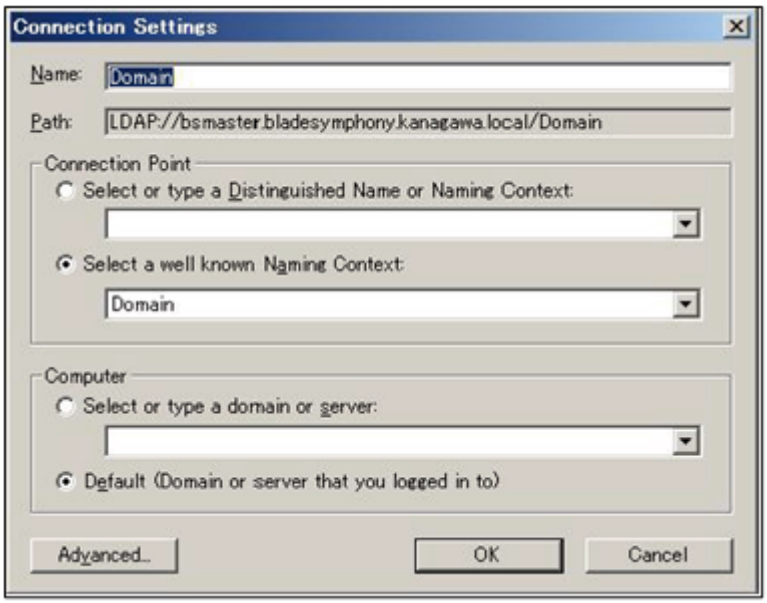
4. スナップインの追加と削除画面に"ADSI Edit"が追加されたら，［OK］ボタンをクリックしてください。

   MMC 画面の［コンソールルート］に［ADSI Edit］が追加されたことを確認します。



5. MMC 画面の［ADSI Edit］にマウスを合わせて右クリックし，"Connect to ..."を選択してください。

6. 接続する Active Directory のドメインのコンテキストが選べるので，［Domain］を選び［OK］ボタンをクリックしてください。



7. ADSI Edit のツリーを展開し，LDAP ディレクトリ上のロールを付与するユーザアカウントを右クリックし，［プロパティ］を開きます。
8. プロパティを開くと，ユーザアカウントに割り当てられている Attribute の一覧が表示されます。
9. Attribute の一覧から，Syntax が"Unicode String"であり，かつ Value が"<Not Set>"のものを選択し，［Edit］ボタンをクリックしてください。
10. マネジメントモジュール用ロールを設定してください。

    マネジメントモジュール用ロール設定は次の形式の文字列で入力します。

    ```
    ManagementModuleRole=role_name
    role_name はマネジメントモジュールに定義されているロール名となります。
    ```

11. ロール設定の入力後，［OK］ボタンをクリックしてください。
12. プロパティに戻った後，［OK］ボタンをクリックしてください。

以上で，マネジメントモジュールのロール設定は完了します。

(4) グループ登録

グループ認証に使用するグループの登録を行います。

参考 グループ認証を使用しない場合は，本項目の設定は不要です。

［管理ツール > Active Directory ユーザーとコンピュータ］を開き，LDAP ディレクトリ上にマネジメントモジュールにログインを許可するグループを作成します。グループの作成後，ログインを許可するユーザアカウントをグループに登録します。

グループの作成およびユーザアカウントのグループへの登録方法については，お使いの Windows Server のドキュメントを参照してください。

(5) Windows Support Tools について

Windows Support Tools は，Active Directory に登録されているオブジェクトの操作を行う「ADSI（Active Directory Service Interface） Edit」および Active Directory に対して LDAP 経由で操作を実行する「ldp」が含まれたパッケージです。

ここでは，本パッケージがインストールされているかの確認方法について述べます。

参考 Windows Server 2008 以降を利用する場合は，標準でインストールされていますので，本手順は不要です。

［コントロールパネル > プログラムの追加と削除］を開くと，インストール済みプログラムの一覧が表示されます。この一覧中に，「Windows Support Tools」が表示されている場合は，「ADSI Edit」および「ldp」は使用可能な状態です。

表示されていない場合は，Windows Support Tools を Windows Server のインストールメディアからインストールしてください。

2.16.4 マネジメントモジュールへの設定

LDAP 連携を行う際に，マネジメントモジュールに行う設定は次のとおりです。

- LDAP 連携設定

  LDAP 連携を行うかどうかの設定が可能です。

  システム装置出荷時は無効になっています。

  本設定を有効にすることで，ユーザ認証時に LDAP サーバ上の LDAP ディレクトリを検索し，認証を試みるようになります。

- LDAP 連携有効時の認証方式設定

  LDAP 連携を行う場合の認証方式については「2.16.1 概要」を参照ください。

- LDAP サーバ登録

  LDAP サーバを最大 3 台登録します。

  LDAP サーバは，IP アドレス，ホスト名のどちらでも設定可能です。

- LDAP サーバ接続設定

  各設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

  - ポート番号
  - バインド DN，バインドパスワード

    「2.16.3 Active Directory の設定(Windows 側の設定)」で設定した内容に準じて設定を行う必要があります。

- LDAP ディレクトリ検索設定

  LDAP ディレクトリ検索に必要な次の情報を設定します。

  各設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

  - ベース DN
  - ログイン ID を表す属性
  - ロールを表す属性

    「ロール情報付与」でユーザアカウントにロールを付与した場合は，ロール付与に使用した Attribute を指定します。

  LDAP ディレクトリ検索に必要な次の情報を設定します。

  - 照会回数

- グループ認証設定

  グループ認証を行う場合は，次の情報を設定します。

  グループ認証を行わない場合は，本設定は不要です。

各設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

- グループ認証方式

  グループ認証を行わない場合では，LDAP 連携を行う設定なら，LDAP 連携有効時の認証方式設定に従い，個々のモジュールに登録されたアカウント，もしくは LDAP ディレクトリ上のアカウントでユーザ認証を実施します。

  グループ認証を行う場合では，次の 2 つのグループ認証方式を選択できます。

  ・スタティックグループ認証方式

  ・ダイナミックグループ認証方式

  前者の認証方式ならば，後述するログインを許可する DN に認証対象のユーザアカウントが所属しているか否かを確認する方法で認証を行います。後者の認証方式ならば，後述する検索フィルタに設定された条件に当てはまるすべてのユーザアカウントの中に認証対象のユーザアカウントが含まれるか否かを確認する方法で認証を行います。

- グループを表す属性

参考 ログインを許可する DN にユーザアカウントが所属しているか否かを tokenGroups 属性もしくは gidNumber 属性で判別できる LDAP ディレクトリを利用する場合は本設定項目の設定が不要となります。

- ログインを許可する DN

  「(4) グループ登録」で作成したグループの DN を指定します。

- ログインを許可する DN のロール
- ダイナミックグループの検索 DN
- ダイナミックグループの検索フィルタ
- ダイナミックグループのロール

表 2-97 Web コンソールでの操作方法

項目	画面
LDAP 連携設定の表示，設定	Administration タブ → LDAP

表 2-98 CLI コンソールでの操作方法

項目	コマンド
LDAP 連携設定の表示	show user ldap
LDAP サーバの登録，変更	set user ldap server
LDAP 連携設定の初期化	clear user ldap
LDAP ディレクトリ検索設定の設定	set user ldap search
LDAP グループ認証設定の設定	set user ldap group

2.17 RADIUS 認証

マネジメントモジュールにおける RADIUS 認証について説明します。

2.17.1 概要

本システム装置では Remote Authentication Dial In User Service (以降 RADIUS)を用いてユーザ認証を行うことができます。

RADIUS 認証を利用する場合，ユーザ認証時に RADIUS サーバでの認証結果を元に，ログイン可否を判断します。RADIUS サーバにユーザアカウント情報を追加することで, RADIUS 認証を利用するすべてのモジュールにおいて，追加されたユーザアカウントでのログインが可能となり，個々のモジュールにユーザアカウント情報を登録する必要がなくなります。

RADIUS 認証を行う場合，次の二つの認証方式を利用することができます。

- 個々のモジュールに登録されたユーザアカウントでのユーザ認証を先に実施し, 認証に失敗した場合に RADIUS サーバにてユーザ認証を実施する方式
- RADIUS サーバのみでユーザ認証を実施する方式

RADIUS サーバは最大 3 台登録することができます。複数登録した場合は，ユーザ認証実行時に登録順に RADIUS サーバへ接続を試みます。最初に接続に成功した RADIUS サーバにおいてユーザ認証を試みます。登録したすべての RADIUS サーバへの接続に失敗した場合は, ユーザ認証は失敗します。

2.17.2 サポートする RADIUS サーバ

本システム装置では，次に示す Windows Server の Network Policy Server もしくは FreeRADIUS を用いた RADIUS 認証をサポートします。

- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Datacenter
- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 Standard
- Windows Server 2008 Enterprise

2.17.3 RADIUS サーバへの設定

RADIUS 認証を用いる場合，マネジメントモジュールを RADIUS クライアントとして登録しておく必要があります。

RADIUS クライアント登録方法については, RADIUS サーバのマニュアルを参照するようお願いいたします。

2.17.4 マネジメントモジュールへの設定

RADIUS 認証を行う際，マネジメントモジュールに行う設定は次のとおりです。

設定操作については「*BladeSymphony BS500 Web コンソールユーザーズガイド*」を参照してください。

- RADIUS 認証設定

  RADIUS 認証を行うかどうかの設定が可能です。

  システム装置出荷時は無効になっています。

  本設定を有効にすることで，ユーザ認証時に RADIUS 認証を試みるようになります。

  ［注意］LDAP 連携と RADIUS 認証を同時に利用することはできません。

  RADIUS 認証を利用する場合は，LDAP 連携設定を無効に設定してください。

- RADIUS 認証有効時のユーザ認証方式設定

  RADIUS 認証を行う場合の認証方式については「2.17.1 概要」を参照ください。

- RADIUS 認証ユーザのロール

  RADIUS サーバでのユーザ認証でログインしたユーザに付与するロールを設定することができます。

- RADIUS サーバ登録

  RADIUS サーバを最大 3 台登録できます。下記の項目は登録する RADIUS サーバ毎に設定します。

  - サーバ名

    IP アドレス(IPv4/IPv6)，ホスト名のどちらでも設定可能です。

  - shared secret

    RADIUS サーバとマネジメントモジュールが共有するパスワードです。

    RADIUS サーバと同じ値を設定する必要があります。

    32 文字以上の長さおよび英数記号が含まれる難解なパスワードを利用することを推奨します。

  - 認証方式

    RADIUS サーバでユーザ認証を行う際に用いる認証方式です。

    PAP, CHAP, MS-CHAPv2 から選択することができます。

  - ポート番号

    RADIUS サーバとの通信に用いるポート番号を指定します。ここで指定されたポート番号宛に通信を試みます。

  - タイムアウト時間

    RADIUS サーバとの通信時に，ここで指定された時間内に RADIUS サーバから応答がない場合，通信失敗と扱います。再送回数が設定されている場合は，再送を行います。

  - 再送回数

    RADIUS サーバとの通信でタイムアウトが発生した場合に，ここで指定された回数の再送を行います。再送を行っても RADIUS サーバから応答がない場合は，次に登録されている RADIUS サーバとの通信を試みます。登録されているすべての RADIUS サーバとの通信に失敗した場合は，認証失敗となります。

2.17.5 RADIUS サーバ接続確認

RADIUS サーバとの接続を確認することができます。

操作については「*BladeSymphony BS500 Web コンソールユーザーズガイド*」を参照してください。

RADIUS サーバ登録で設定した RADIUS サーバに対して，ユーザ認証を試み，認証結果を表示します。接続確認を実施する際，ユーザアカウントおよびパスワードを指定する必要があります。

2.18 Web コンソールにおけるデジタル証明書の利用

Web コンソールにおけるデジタル証明書について説明します。

2.18.1 概要

デジタル証明書を利用して次の機能を実現できます。自己署名証明書およびお客様ご自身で用意した認証局に署名された証明書を使用することができます。

- マネジメントモジュールの認証

Web コンソールを利用する際，マネジメントモジュールからデジタル証明書が提示されます。デジタル証明書に署名した認証局を確認することで，マネジメントモジュールを認証できます。

- Web ブラウザとマネジメントモジュールとの通信の暗号化

  Web コンソールを利用する際に通信を暗号化し，盗聴や改ざんを防ぎます。

- BMC の認証

  サーバブレードの Web コンソールまたはリモートコンソールを利用する際，BMC からデジタル証明書が提示されます。

  デジタル証明書に署名した認証局を確認することで BMC を認証できます。

- Web ブラウザ，リモートコンソールと BMC との通信の暗号化

  サーバブレードの Web コンソールまたはリモートコンソールを利用する際に通信を暗号化し，盗聴や改ざんを防ぎます。

2.18.2 デジタル証明書利用の諸元

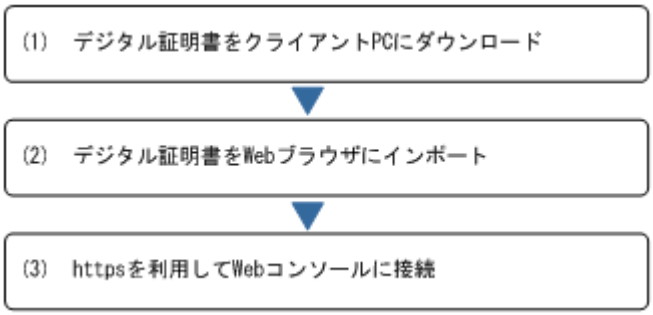
Web コンソールにおけるデジタル証明書利用の諸元を次に示します。

表 2-99 Web コンソールにおけるデジタル証明書利用の諸元

項目	内容
公開鍵アルゴリズム・ビット長	RSA(2048bit)
インポート可能な証明書の形式	PEM 形式
ダウンロード時の証明書の形式	PEM 形式
作成可能な証明書の形式	PEM 形式
証明書に記入可能な発行対象の情報	「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。

2.18.3 デジタル証明書利用の手順(自己署名証明書を使用する場合)

操作の流れは次のとおりです。



(1) デジタル証明書をクライアント PC にダウンロード

自己署名されたデジタル証明書は，マネジメントモジュール，サーバブレードの出荷時に既に作成されています。Web ブラウザから，デジタル証明書をお客様のクライアント PC にダウンロードしてください。Web ブラウザからのデジタル証明書のダウンロード方法は，Web ブラウザのヘルプを参照してください。

(2) ダウンロードしたデジタル証明書を Web ブラウザにインポート

手順（1）でダウンロードしたサーバ証明書を，お客様のクライアント PC の Web ブラウザにインポートしてください。Web ブラウザのインポートの方法は，Web ブラウザのヘルプを参照してください。

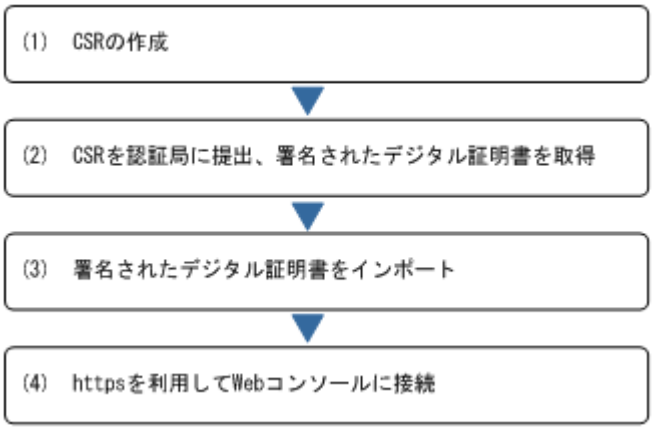
(3) HTTPS を利用して Web コンソールに接続

HTTPS を利用して，Web コンソールに接続してください。

通信経路の暗号化機能が利用可能になります。

2.18.4 デジタル証明書利用の手順(認証局に署名されたデジタル証明書を使用する場合)

操作の流れは次のとおりです。



(1) CSR の作成

Web コンソールから，CSR の作成を実施してください。CSR 作成時に入力する項目は「2.18.2 デジタル証明書利用の諸元」を参照してください。

(2) CSR を認証局へ提出・署名されたデジタル証明書を取得

作成した CSR を認証局へ提出し，署名されたデジタル証明書を取得してください。

(3) 署名されたデジタル証明書をインポート

Web コンソールから，（2）で署名されたデジタル証明書をインポートしてください。

表示されるデジタル証明書の情報が，お客様が取得したデジタル証明書の情報と一致することを確認して，インポートを実施してください。インポートに失敗した場合は，再度（1）の CSR 作成から再実施してください。

(4) HTTPS を利用して Web コンソールに接続

HTTPS を利用して，Web コンソールに接続してください。

通信経路の暗号化機能が利用可能になります。マネジメントモジュールの認証機能を有効とするためには，認証局のルート証明書がお客様のクライアント PC の Web ブラウザにインポートされている必要があります。確認方法については，Web ブラウザのヘルプおよび認証局に確認してください。

重要 マネジメントモジュールにインポートするデジタル証明書の文字コードは，utf-8 以外としてください。utf-8 とした場合，デジタル証明書のインポート後に表示されるデジタル証明書の情報が，一部表示されないことがあります。

表 2-100 Web コンソールでの操作方法

項目	画面	
マネジメントモジュール	CSR の作成	Administration タブ → 証明書
	証明書のインポート	Administration タブ → 証明書
BMC	CSR の作成	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → BMC タブ → 編集 → 証明書設定
	証明書のインポート	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x → BMC タブ → 編集 → 証明書設定

2.19 HVM 連携

ここでは，Web コンソールを使用した HVM 関連機能についての説明をします。

本機能を利用することで，HVM の導入から構築・運用に至るまでの設定を行うことができます。なお，本節に入る前に次の設定を確認してください。

- サーバブレードの設定
- システム装置へのケーブル接続
- EFI の設定

これらの設定については「*BladeSymphony BS500 サーバブレードセットアップガイド*」を参照してください。

次の表は，Web コンソールと Virtage Navigator の機能一覧を示します。Web コンソールでサポートされていない機能については，Virtage Navigator で設定してください。

表 2-101 Web コンソールと Virtage Navigator の機能一覧

機能		Web コンソール	Virtage Navigator V02-04～
「2.19.1 HVM 初期設定」		○	×
NTP による HVM システム時刻の時刻合わせ		×	○
「2.19.2 HVM ファームウェアの選択」		○	×
「2.19.3 仮想 WWN の確認」		○ ※1	○
「2.19.4 仮想 MAC アドレスの確認」		○ ※2	○
「2.19.5 電源の投入」		○	×
「2.19.6 LPAR 作成」		○ ※3	○
	LPAR 追加	○ ※3	○
	プロセッサ数の設定	○ ※3	○
	メモリサイズの設定	○ ※3	○
	共有 NIC の設定	○ ※3	○
	共有 FC HBA の設定	○ ※3	○
	ブート設定	○ ※4	○
	USB の設定	○ ※3	○
「2.19.7 HVM 構成情報の保存」		○	○
「2.19.8 LPAR への USB 割り当ての設定」		○	○
「2.19.9 LPAR のブートオーダ設定」		○	○
「2.19.10 LPAR の Activate」		○	○

機能	Web コンソール	Virtage Navigator V02-04～
「2.19.11 リモートコンソールの呼び出し」	○	○
「2.19.12 LPAR の Reactivate」	○	○
「2.19.13 LPAR の Deactivate」	○	○
「2.19.15 LPAR の削除」	○	○
「2.19.16 HVM の再起動」	○	○
「2.19.17 HVM のシャットダウン」	○	○
「2.19.18 HVM 設定のバックアップ」	○	×
「2.19.19 HVM 設定のリストア」	○	×
「2.19.20 HVM 設定の初期化」	○	×
「2.19.21 HVM のモデルアップ」(※5)	○	×
HVM ファームウェアのバージョンアップ(※6)	○	×
「2.19.22 HVM ファームウェアのアップデート」	○	×
HVM ファームウェアのバージョンダウン	○ ※7	×
HVM ファームウェアのリビジョンダウン	○ ※7	×
HVM スクリーンの呼び出し	×	○
Web コンソールの呼び出し	−	○
Virtage Navigator の呼び出し	×	−
モニタリング	×	○
構成ビューア(HVM システム構成の図表表示)	×	○
LPAR マイグレーション	×	○
「2.19.24 HVM 稼働時ダンプの採取」 【マネジメントモジュールファームウェアバージョン A0145 以降】	○	○
HVM ダンプの保存(※8)	○	○ ※9
マネジメントモジュールから，HVM ダンプを出力する (※10) (※11)	○	×

○：設定可　×：設定不可

※1：original WWN の表示のみサポート

※2：original MAC アドレスの表示のみサポート

※3：一部の設定または表示をサポート

※4：Boot Function の設定のみサポート

※5：HVM ライセンスキーを用意する必要あり

※6：バージョンアップキーを用意する必要あり

※7：利用可能。ただし，HVM 構成情報の引き継ぎを保証できません。「2.19.19 HVM 設定のリストア」，「2.19.22 HVM ファームウェアのアップデート」の手順で操作してください。

※8：HVM スクリーンでも利用可能

※9：保守員の指示で利用可能

※10：CLI コンソールでも利用可能

※11：詳細は「2.28 ログ」を参照してください。

なお, Virtage Navigator でサポートされている機能詳細につきましては,「*Virtage Navigator* ユーザーズガイド」を参照してください。

「*Virtage Navigator* ユーザーズガイド」は，BladeSymphony Web ページより入手できます。

BladeSymphony Web ページ:

http://www.hitachi.co.jp/products/bladesymphony/

重要

- HVM ファームウェアのバージョンダウン，または HVM ファームウェアのリビジョンダウンにより，以前利用していた HVM ファームウェアバージョンに戻す場合は，その HVM ファームウェアを利用していた際にバックアップした HVM 構成情報を，リストアしてください。
- Web コンソールで表示される内容は，自動で更新されません。

  Web コンソールで HVM のシャットダウンを実行した場合や他のコンソールによる設定変更を実行した場合は，必ず手動で[更新]ボタンをクリックしてください。更新を行わずに操作をすると，画面上で表示される値が実際の設定値と異なります。

参考 【マネジメントモジュールファームウェアバージョン A0205 以降】
HVM が暗号化通信をサポートしている場合，マネジメントモジュールのセキュリティ強度設定にかかわらず，マネジメントモジュールと HVM 間の制御通信は暗号化されます。

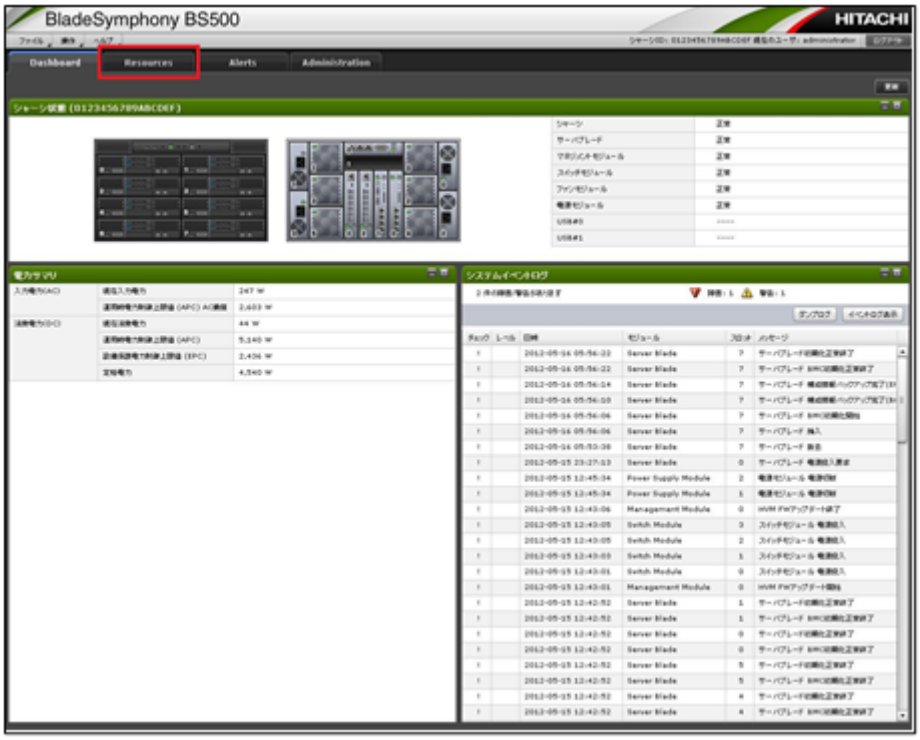
重要 Web コンソールには，マネジメントモジュールやサーバブレードなどファームウェアのバージョン要件を満たさないと，一部実行できない機能があります。

2.19.1 HVM 初期設定

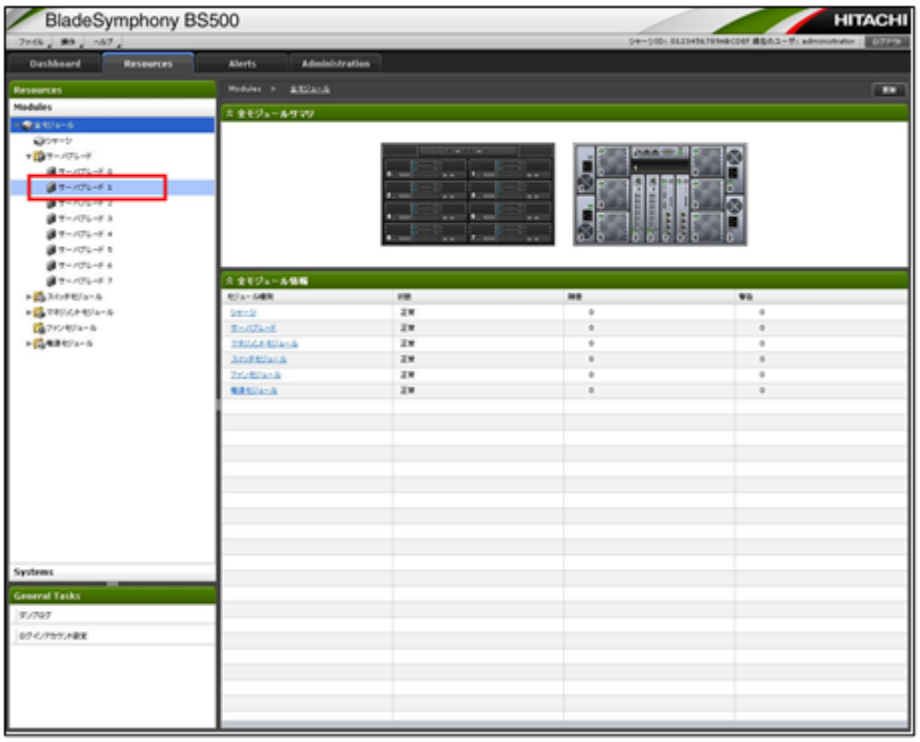
次の手順で HVM の初期設定を実施してください。

【マネジメントモジュールファームウェアバージョン A023X 以前】

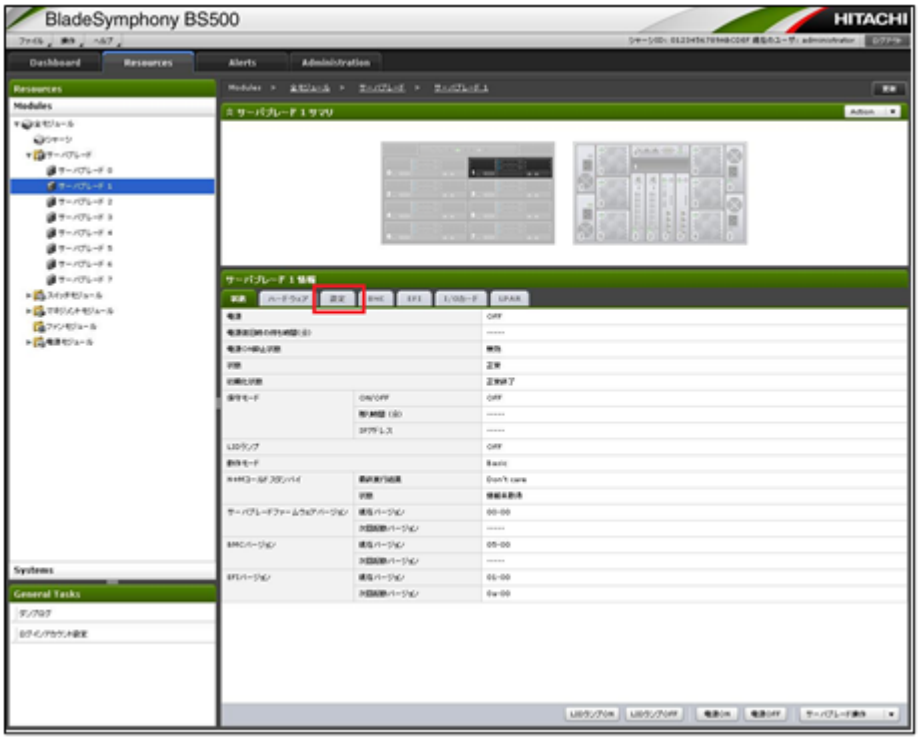
1. [Resources]タブをクリックします。



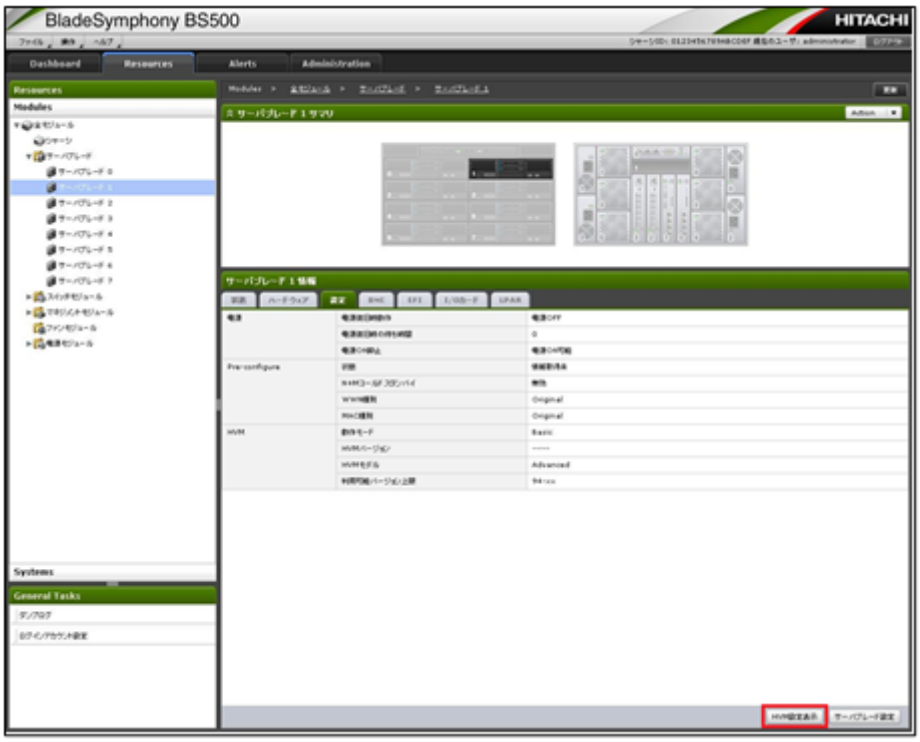
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



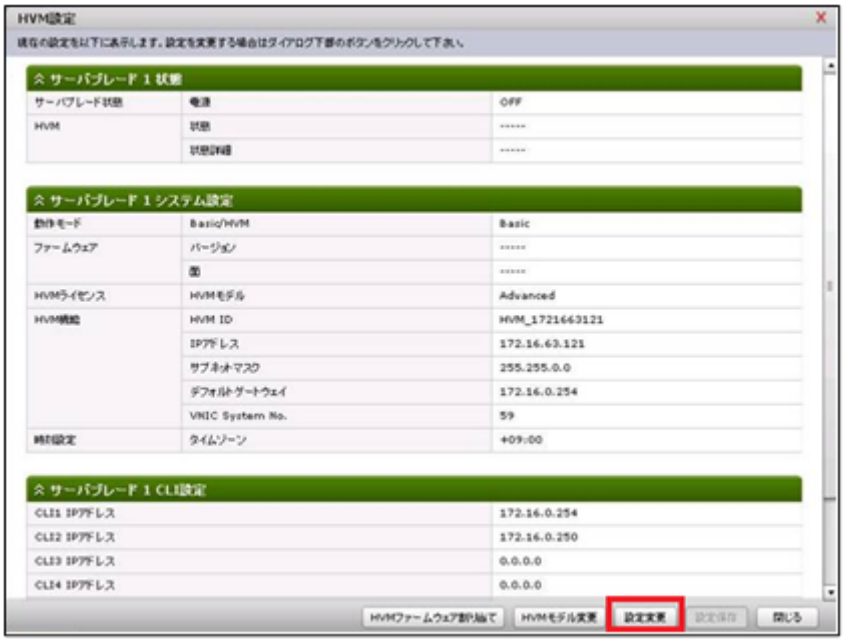
3. [サーバブレード]パネルの[設定]タブを選択します。



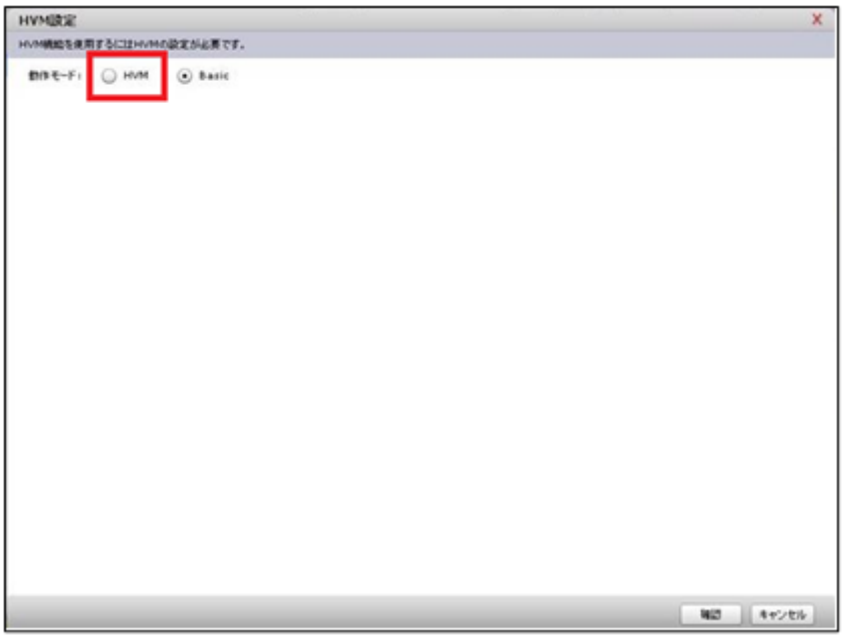
4. [HVM 設定表示]ボタンをクリックします。



5. [HVM 設定]ダイアログが表示されます。
   [設定変更]ボタンをクリックします。



6. [動作モード]で[HVM]ラジオボタンを選択します。



7. 「IP アドレス」,「サブネットマスク」,「デフォルトゲートウェイ」,「VNIC System No.」,および「タイムゾーン」を入力してください。

   「HVM ID」は，入力必須項目ではありませんが，入力することを推奨します。

重要

- VNIC System No.は，共有 NIC および仮想 NIC の MAC アドレスの重複を防ぐため，MAC アドレス生成に使用されます。BladeSymphony シリーズの HVM システムにユニークな値を設定してください。

  【マネジメントモジュールファームウェアバージョン A0135 以前】

  1～128 の範囲で指定します。

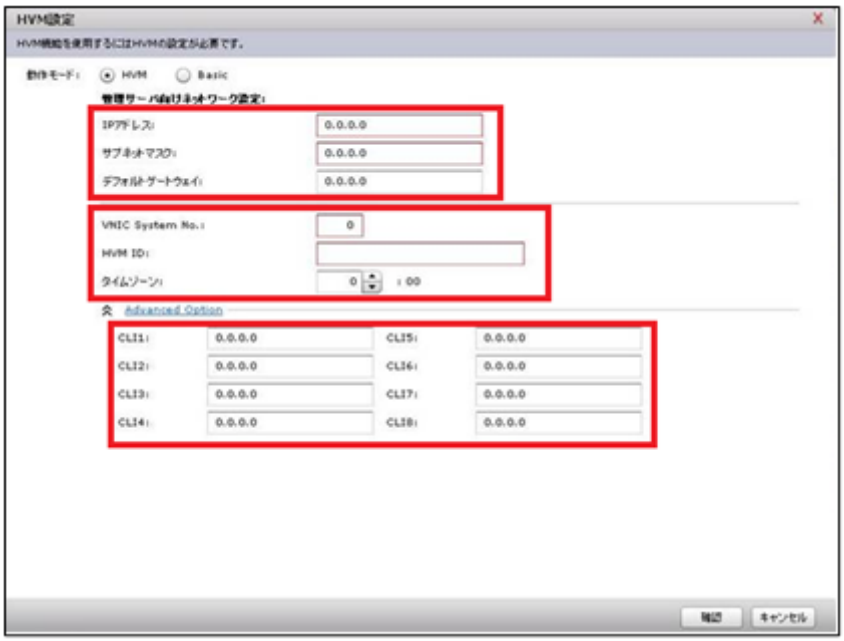
  【マネジメントモジュールファームウェアバージョン A0145 以降】

  1 以上の範囲で指定します。最大値は HVM ファームウェアバージョンによって変化します。

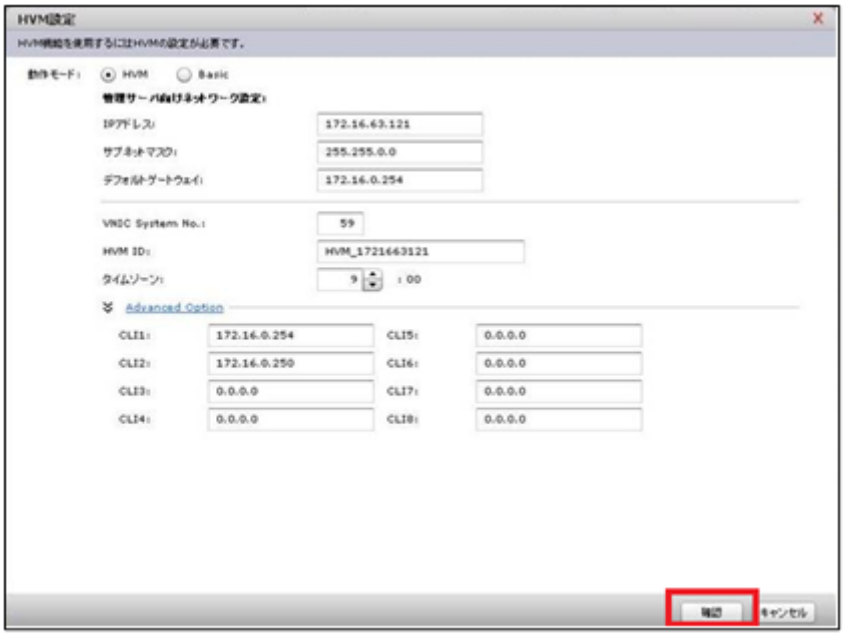
  【サーバブレードに HVM ファームウェアが未割り当ての場合】

  1～128 の範囲で指定します。

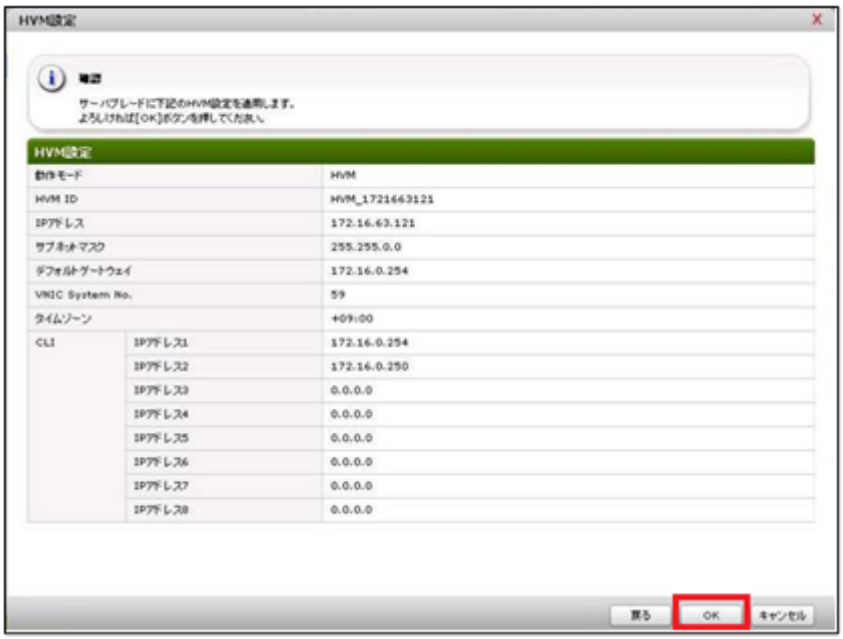
- IP アドレスは，マネジメントモジュールやサーバブレードの IP アドレスなどと重複しないように設定してください。重複して設定した場合は，Web コンソールやリモートコンソールなどに接続できなくなります。
- HVM ファームウェアバージョン 01-5X 以前の場合，HVM とマネジメントモジュールの IP アドレス，デフォルトゲートウェイは，同一ネットワークとなるように設定してください。HVM ファームウェアバージョン 01-60 以降の場合，HVM の IP アドレス，デフォルトゲートウェイは，同一ネットワークとなるように設定してください。
- デフォルトゲートウェイを使用しない場合は，「0.0.0.0」としてください。空白とした場合，HVM の起動に失敗することがあります。



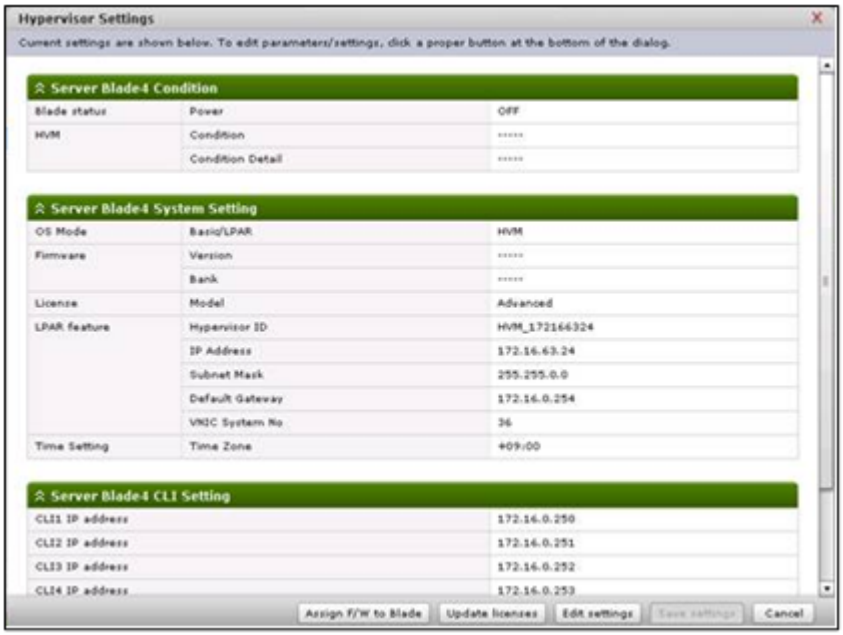
8. [確認]ボタンをクリックします。



9. [OK]ボタンをクリックします。

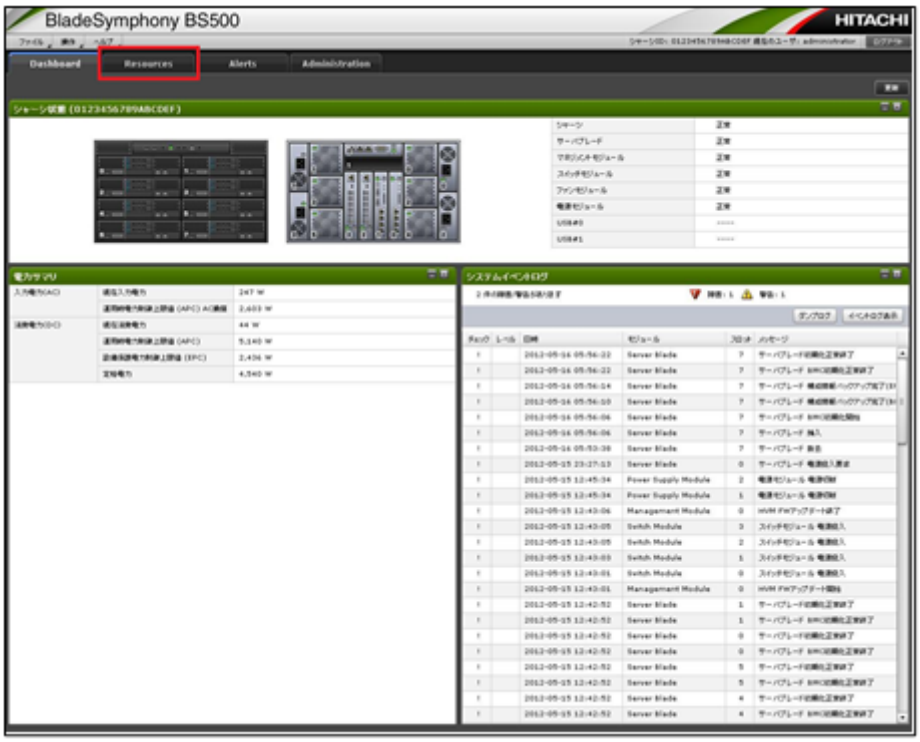


10. [HVM 設定]ダイアログに戻ります。

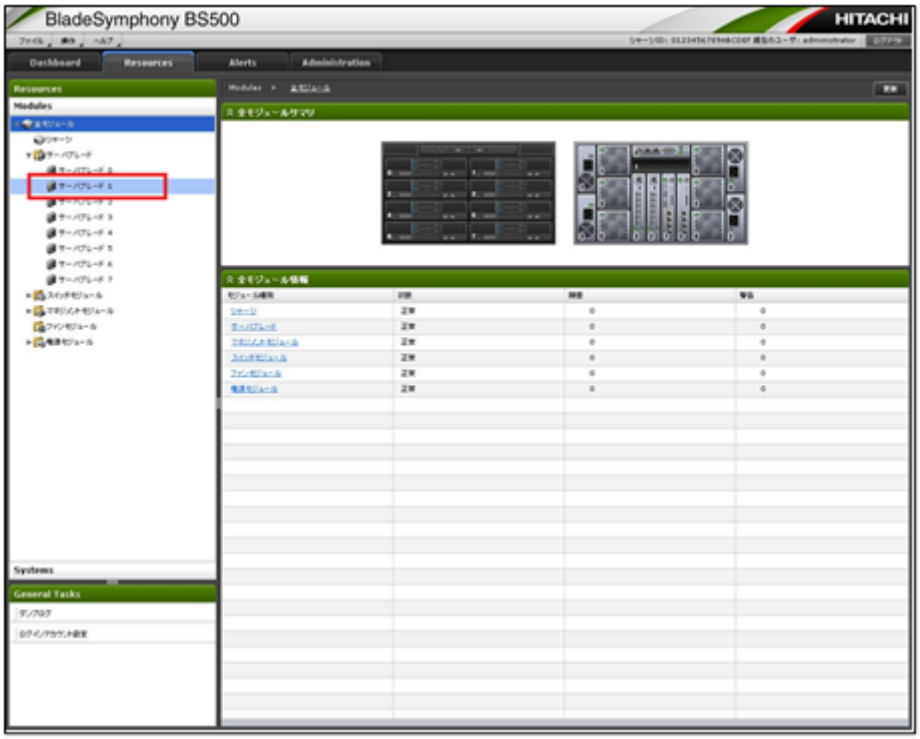


【マネジメントモジュールファームウェアバージョン A0240 以降】

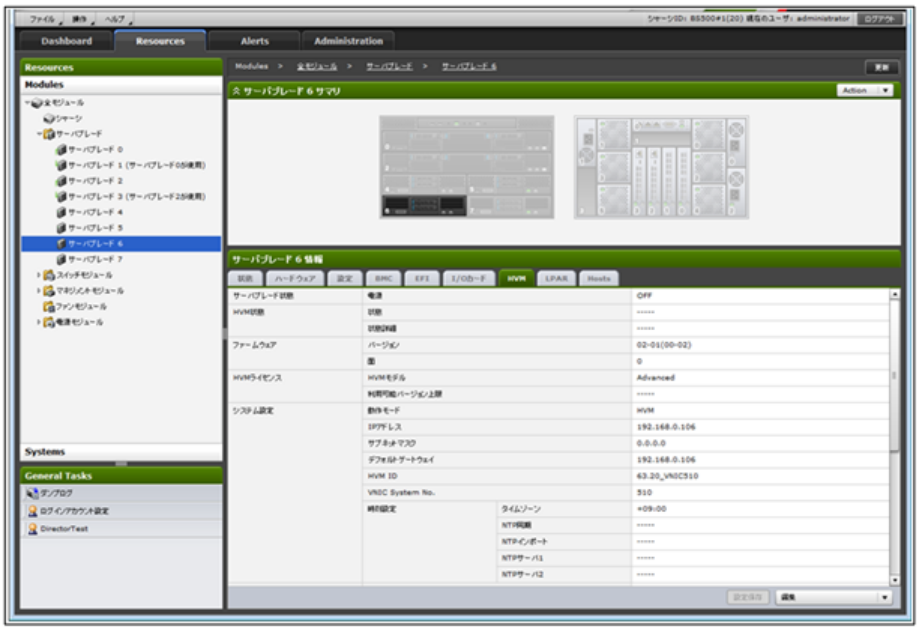
1. [Resources]タブをクリックします。



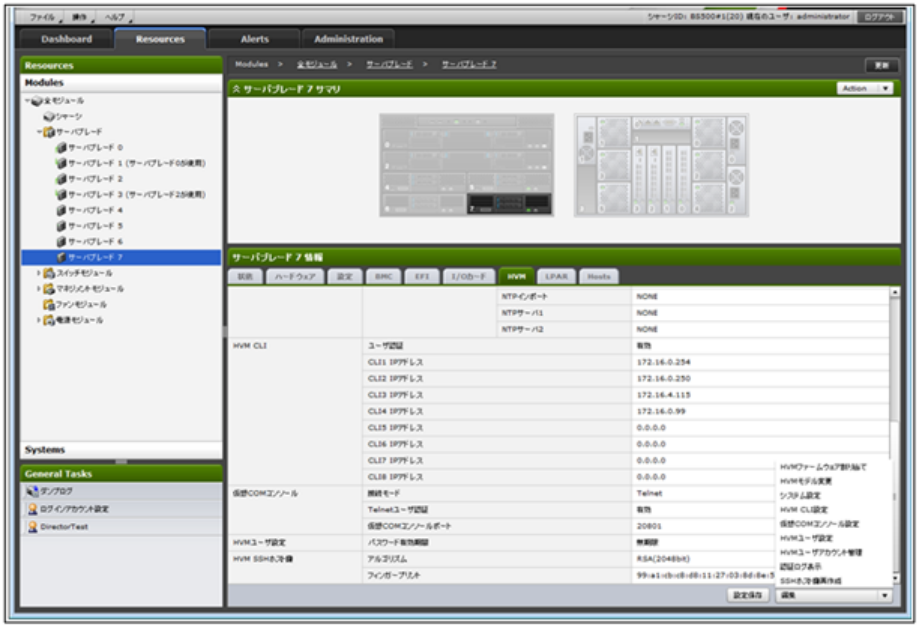
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[HVM]タブを選択します。



4. [編集]ボタン→[システム設定]を選択します。



5. [動作モード]で[HVM]ラジオボタンを選択します。

   IPv4 の IP アドレス，IPv6 のスタティックアドレスのどちらかを設定する必要があります。

   IPv4 の設定は[IPv4]タブの[IP アドレス]，[サブネットマスク]，[デフォルトゲートウェイ]を設定します。

   IPv6 の設定は[IPv6]タブの[スタティックアドレス]で[有効]を選択し，[IP アドレス]，[プレフィックス長]，[デフォルトゲートウェイ]を設定します。[ステートレスアドレス]は HVM の起動には使用しないため必須ではありません。

   [HVM-マネジメントモジュール間通信]で[IPv4]または[IPv6(スタティックアドレス)]を設定します。IPv4 を設定した場合，HVM およびマネジメントモジュールに IPv4 のアドレスが設定されている必要があります。

   IPv6(スタティックアドレス)を設定した場合，HVM およびマネジメントモジュールに IPv6 のアドレスが設定されている必要があります。

   [VNIC System No.]，[タイムゾーン]を設定します。[HVM ID]は必須ではありませんが，設定することを推奨します。

なお，マネジメントモジュールファームウェアバージョン A0245 以降では，管理パスとして使用する NIC とポートを設定することができます。管理 NIC を指定しない場合，1a/1b を管理パスとして使用します。

重要

- VNIC System No.は，共有 NIC および仮想 NIC の MAC アドレスの重複を防ぐため，MAC アドレス生成に使用されます。BladeSymphony シリーズの HVM システムにユニークな値を設定してください。

  VNIC System No.は，1 以上の値を設定してください。最大値は HVM ファームウェアバージョンによって変化します。
- IP アドレスは，マネジメントモジュールやサーバブレードの IP アドレスなどと重複しないように設定してください。重複して設定した場合は，Web コンソールやリモートコンソールなどに接続できなくなります。
- HVM ファームウェアバージョン 01-5X 以前の場合，HVM とマネジメントモジュールの IP アドレス，デフォルトゲートウェイは，同一ネットワークとなるように設定してください。HVM ファームウェアバージョン 01-60 以降の場合，HVM の IP アドレス，デフォルトゲートウェイは，同一ネットワークとなるように設定してください。
- IPv4 でデフォルトゲートウェイを使用しない場合は，「0.0.0.0」としてください。空白とした場合，HVM の起動に失敗することがあります。なお，マネジメントモジュールファームウェアバージョン A0260 以降では，空白とした場合「0.0.0.0」が設定されます。
- 管理パスとして指定できる NIC は，HVM が共有モードをサポートしている NIC です。それ以外の NIC は選択肢に表示されません。
- 運用中の HVM の構成を変更する場合，管理パスに使用する NIC のスケジューリングモードを共有モードに変更してください。占有モードの NIC を指定した場合，次回 HVM 起動時に，スケジューリングモードが共有モードに変更されます。

  NIC が LPAR に割り当てられていた場合，LPAR から NIC の割り当てが解除されます。この場合，HVM はセーフモードで起動し，HVM 構成情報の保存，LPAR の Activate が抑止されます。

  管理パスとして指定した NIC が正しいか確認し，NIC のスケジューリングモードおよび NIC の割り当て状態を確認・変更した後に，セーフモードを解除してください。

6. [確認]ボタンをクリックします。
7. [OK]ボタンをクリックします。

HVM 初期設定はこれで完了です。

「2.19.2 HVM ファームウェアの選択」を実施してください。

2.19.2 HVM ファームウェアの選択

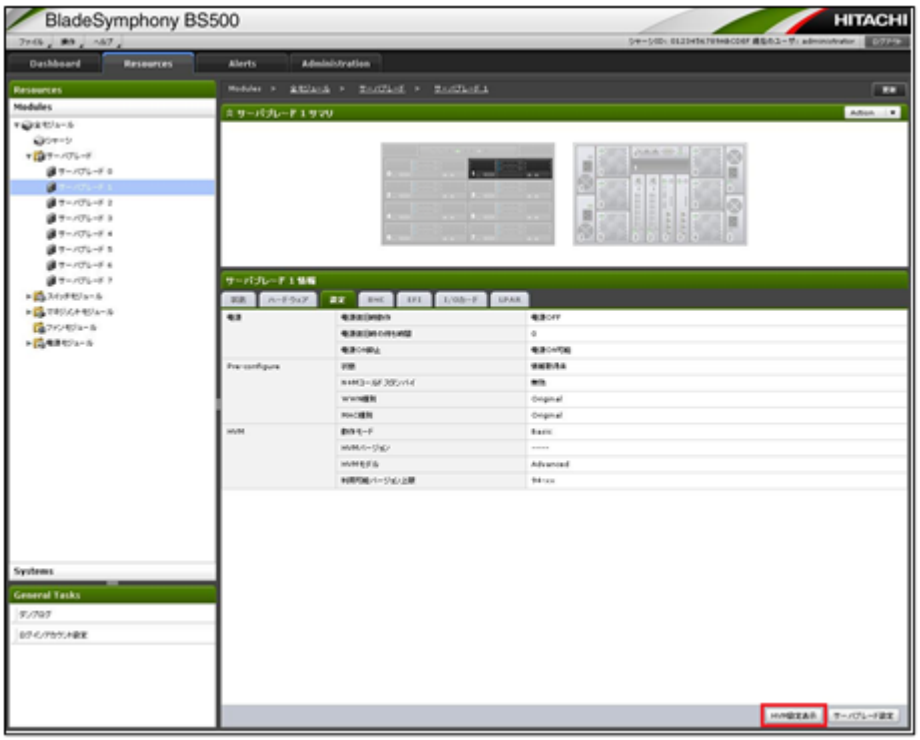
「2.19.1 HVM 初期設定」に続いて，次の手順で HVM ファームウェアの選択を実施してください。

重要

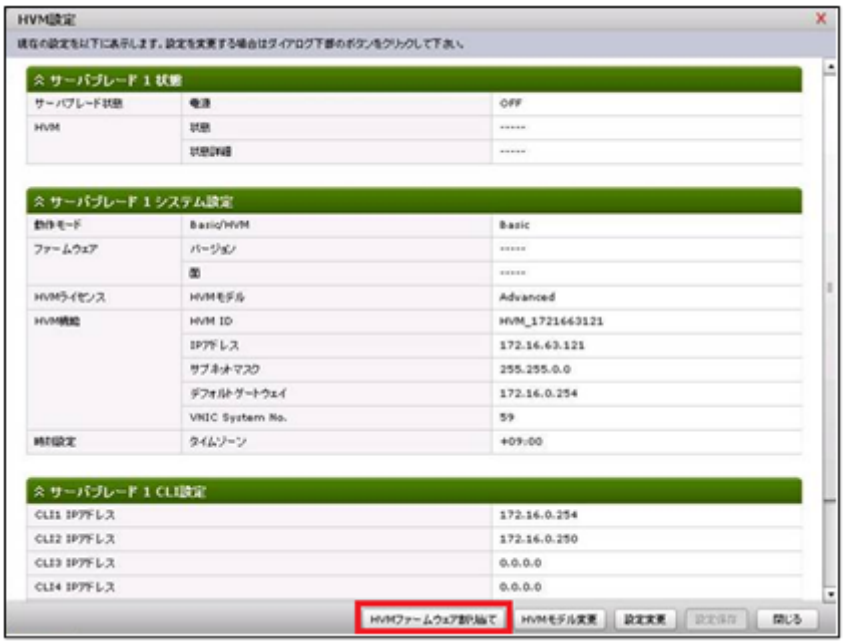
- BS540A サーバブレード A1/B1 に対しては，HVM ファームウェアバージョン 01-10 以降を割り当ててください。HVM ファームウェアバージョン 01-0x を割り当てた場合，サーバブレードは正常に稼働しません。
- SMP 構成の場合，適用される HVM ファームウェアは，プライマリサーバブレードに割り当てられたファームウェアになります。

参考 マネジメントモジュールファームウェアバージョン A0240 以降では，本操作は［HVM］タブで行います。 詳細については，「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。

1. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択後，[サーバブレード]パネルの[設定]タブで[HVM 設定表示]ボタンをクリックします。



2. [HVM ファームウェア割り当て]ボタンをクリックします。



3. HVM ファームウェアを選択し，[次へ]ボタンをクリックします。

参考 サーバブレードに割り当てられている HVM ファームウェアを変更する場合，変更前に現在の構成情報をバックアップすることを推奨します。

構成情報をバックアップしておくと，問題発生時に，変更前の HVM ファームウェアバージョンに戻すことができます。構成情報をバックアップしていない場合，変更前の HVM ファームウェアバージョンに戻すことができません。

構成情報をバックアップする場合は，手順 4 に進みます。

構成情報をバックアップしない場合は，手順 6 に進みます。

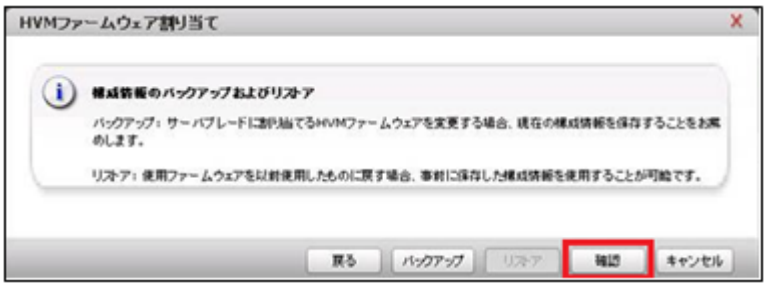
---

4. [バックアップ]ボタンをクリックします。

5. [保存]ボタンをクリックします。

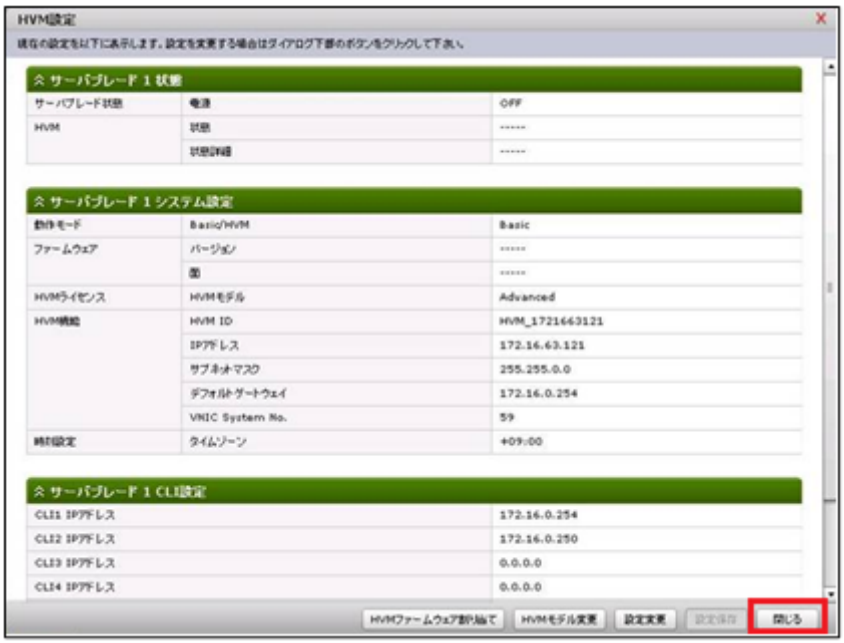
参考 ファイルの保存手順については，OS の操作手順に従ってください。

6. [確認]ボタンをクリックします。



7. [OK]ボタンをクリックします。

8. [閉じる]ボタンをクリックし，[HVM 設定]ダイアログを閉じます。



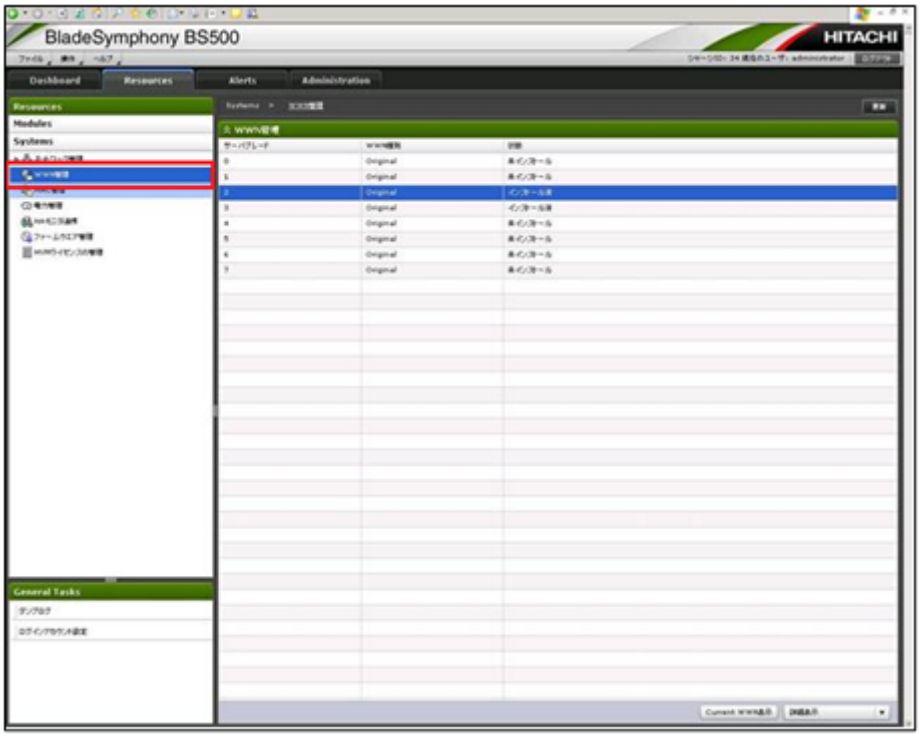
2.19.3 仮想 WWN の確認

LPAR 構築前に，仮想 WWN を確認し，LPAR 構築にお役立てください。

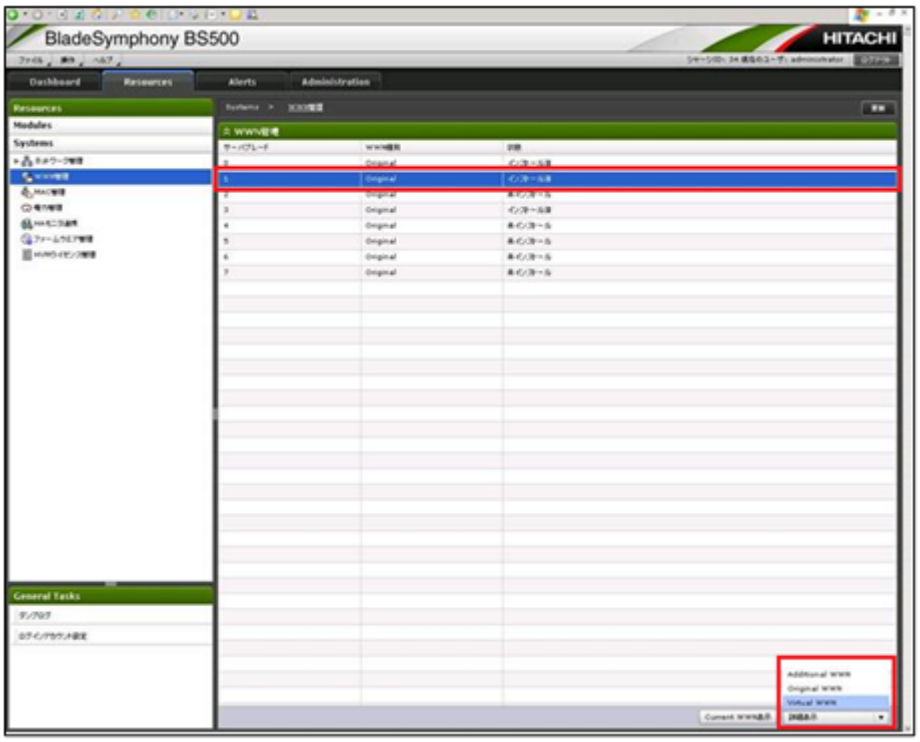
なお，LPAR マイグレーションを実行すると，仮想 WWN は移動してしまいます。

次の手順で仮想 WWN を確認してください。

1. [Resources]パネルの[Systems]アコーディオン内のツリービューから「WWN 管理」を選択します。



2. [WWN 管理]パネルでサーバブレードを選択し，[詳細表示]コンボボックスで[Virtual WWN]を選択します。



3. WWN を確認し，[閉じる]ボタンをクリックします。

参考 データを CSV ファイルに出力することもできます。[CSV 出力]ボタンをクリックしてください。

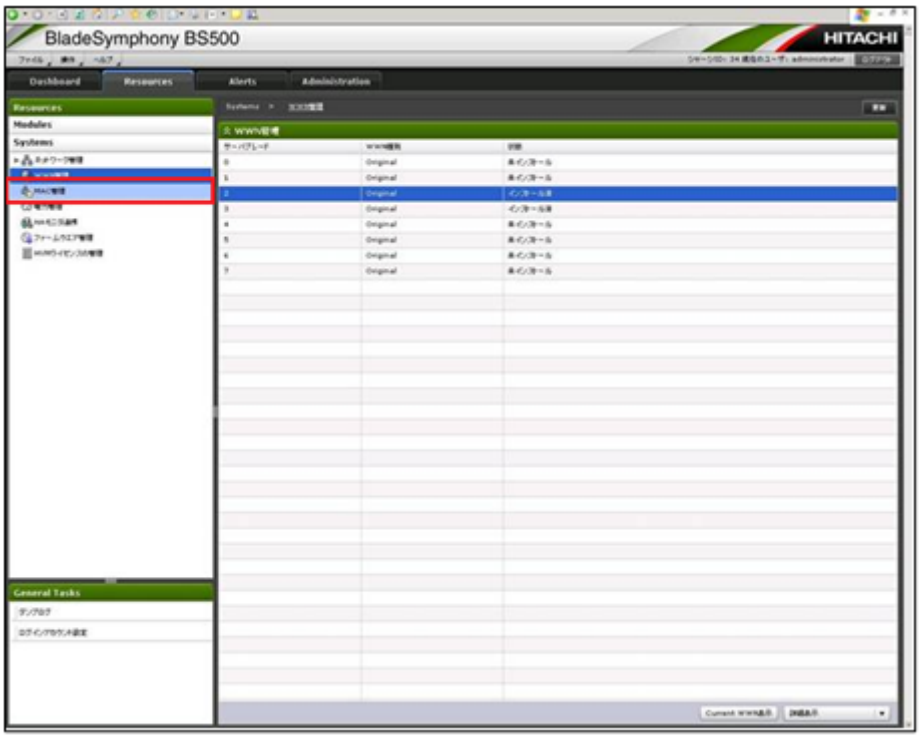
2.19.4 仮想 MAC アドレスの確認

LPAR 構築前に，仮想 MAC アドレスを確認し，LPAR 構築にお役立てください。

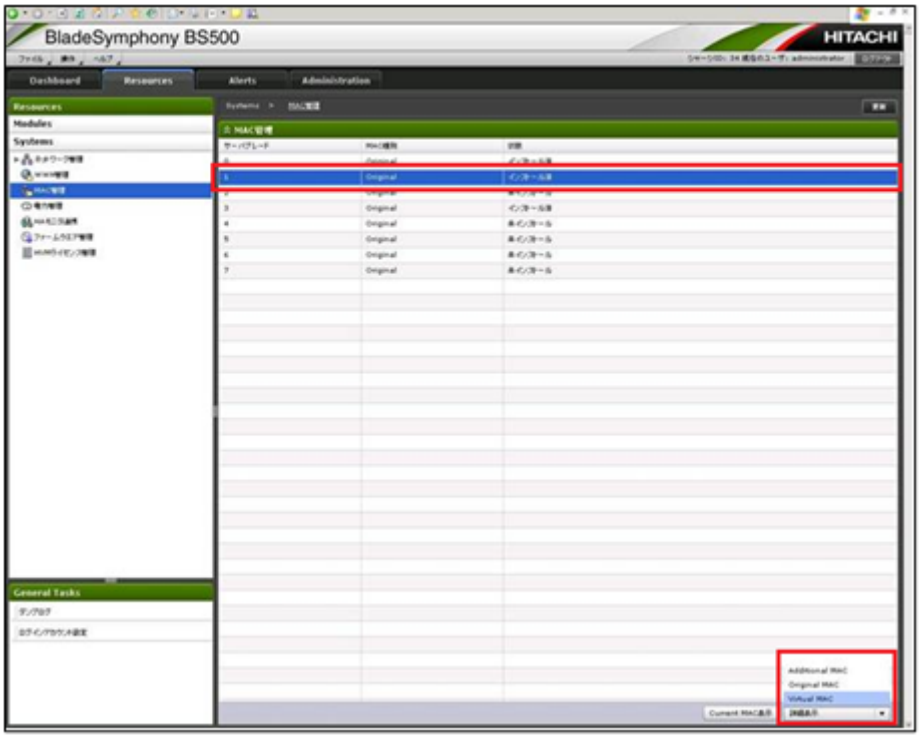
なお，LPAR マイグレーションを実行すると，仮想 MAC アドレスは移動してしまいます。

次の手順で仮想 MAC アドレスを確認してください。

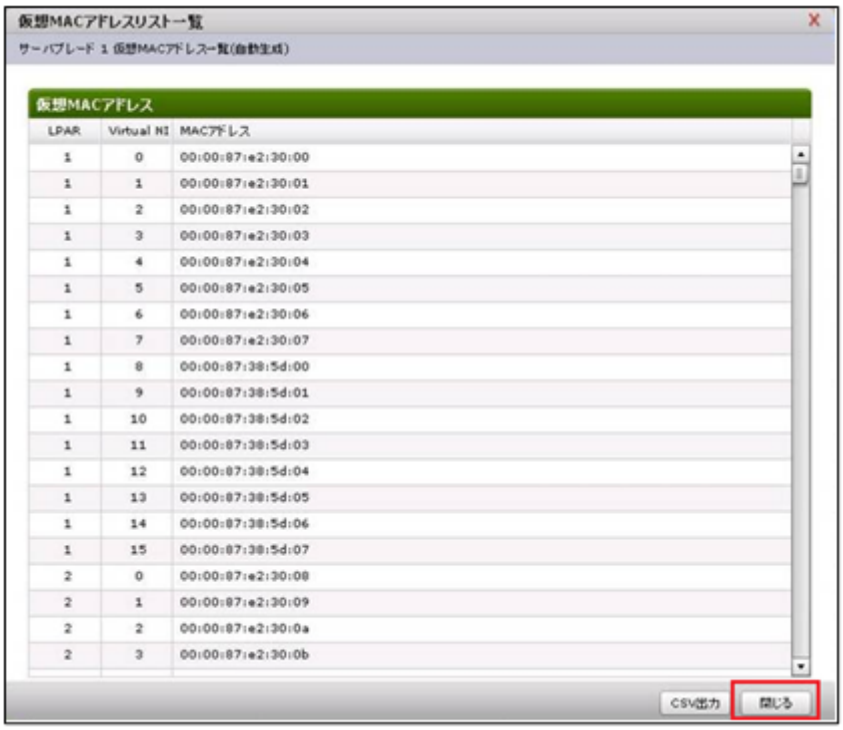
1. [Resources]パネルの[Systems]アコーディオン内のツリービューから「MAC 管理」を選択します。



2. [MAC 管理]パネルでサーバブレードを選択し，[詳細表示]コンボボックスで[Virtual MAC]を選択します。



3. MAC アドレスを確認し，[閉じる]ボタンをクリックします。



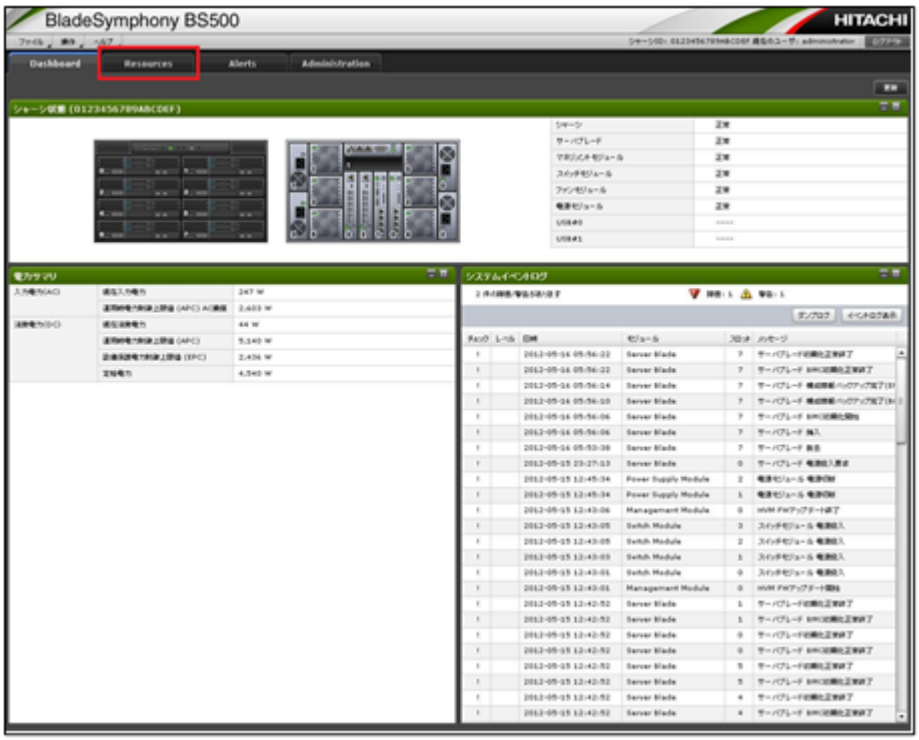
参考 データを CSV ファイルに出力することもできます。[CSV 出力]ボタンをクリックしてください。

2.19.5 電源の投入

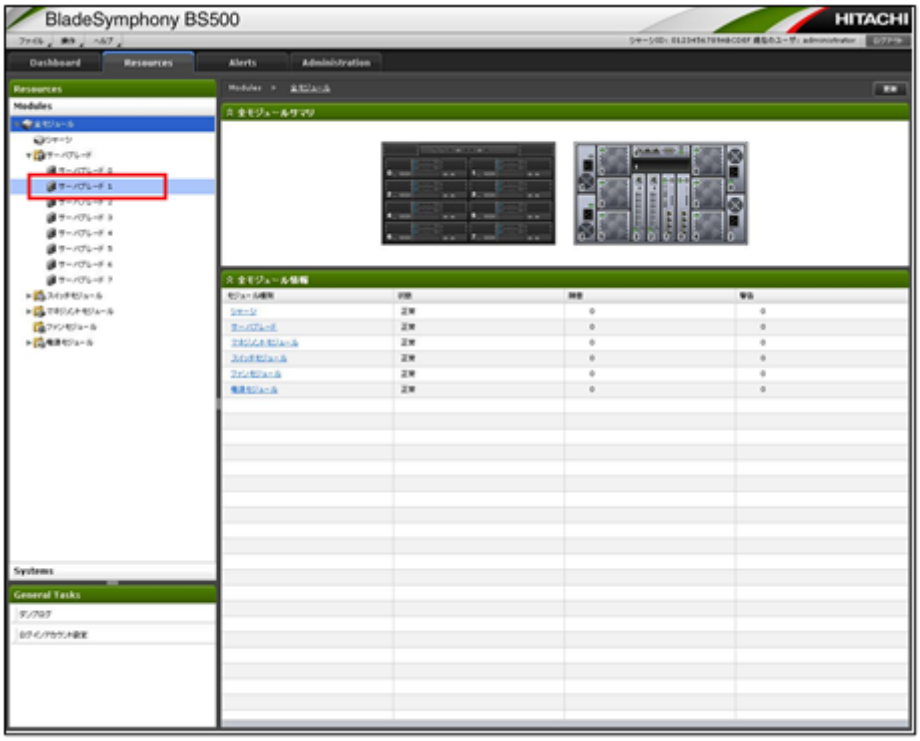
サーバブレードに電源を投入する手順を説明します。

なお，電源を投入してからサーバブレードが起動するまでは，10～15 分程度かかります。サーバブレードの構成により，起動時間は変わる場合があります。

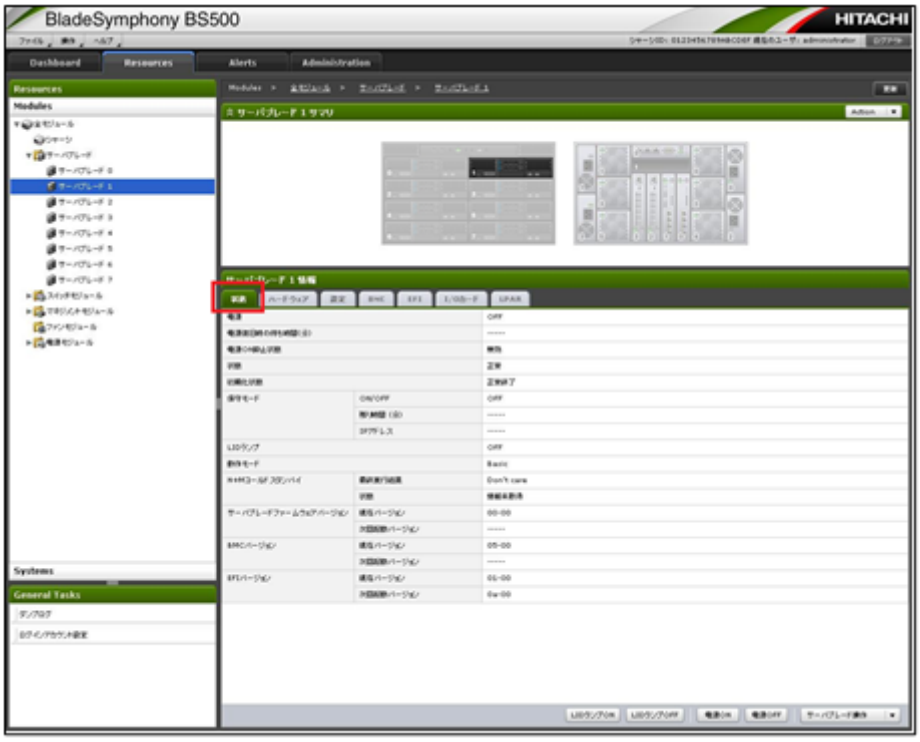
1. [Resources]タブをクリックします。



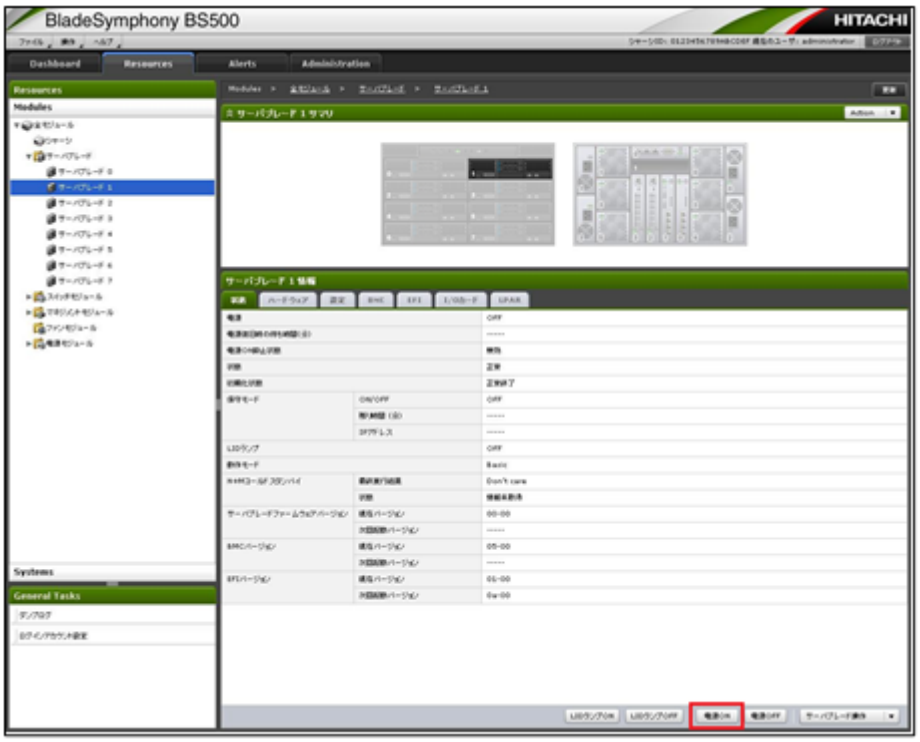
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



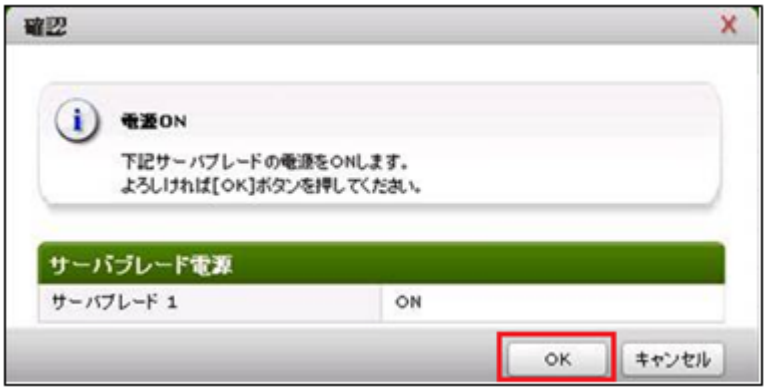
3. [サーバブレード情報]パネルの[状態]タブを選選択します。



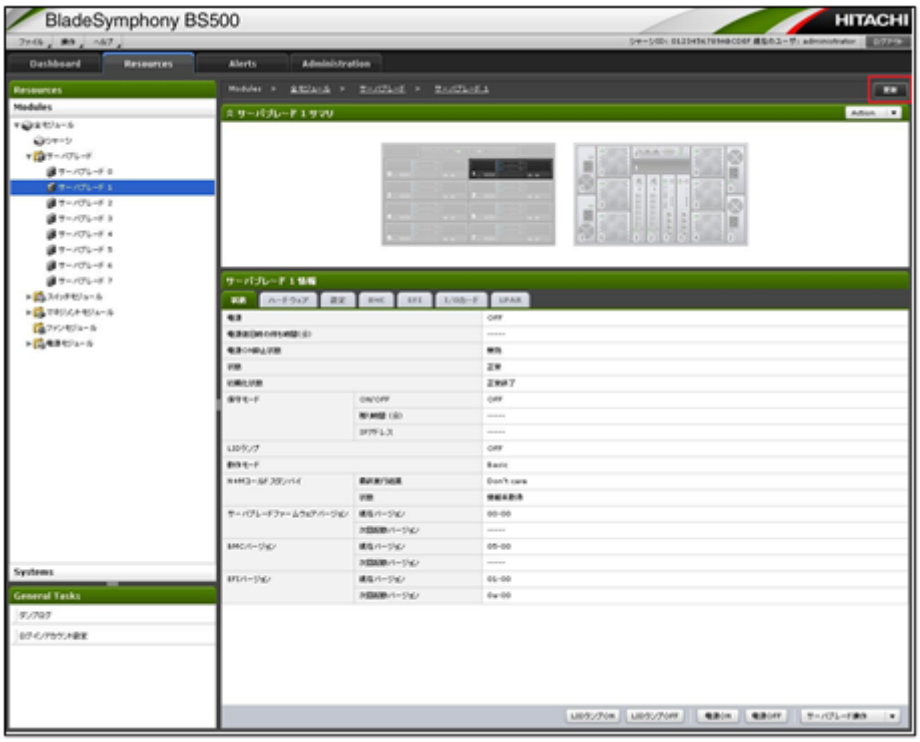
4. [電源 ON]ボタンをクリックします。



5. [OK]ボタンをクリックします。



6. サーバブレード起動後，[更新]ボタンをクリックします。



重要 電源 ON 指示後，HVM の起動が完了するまでの間は，LPAR タブ内に HVM の起動状態が表示されます。([更新]ボタンをクリックすることで，内容が更新されます）ただし，電源投入直後は，次のメッセージが表示されます。

- 状態取得に失敗したことを意味するメッセージ
- HVM シャットダウン中を意味するメッセージ

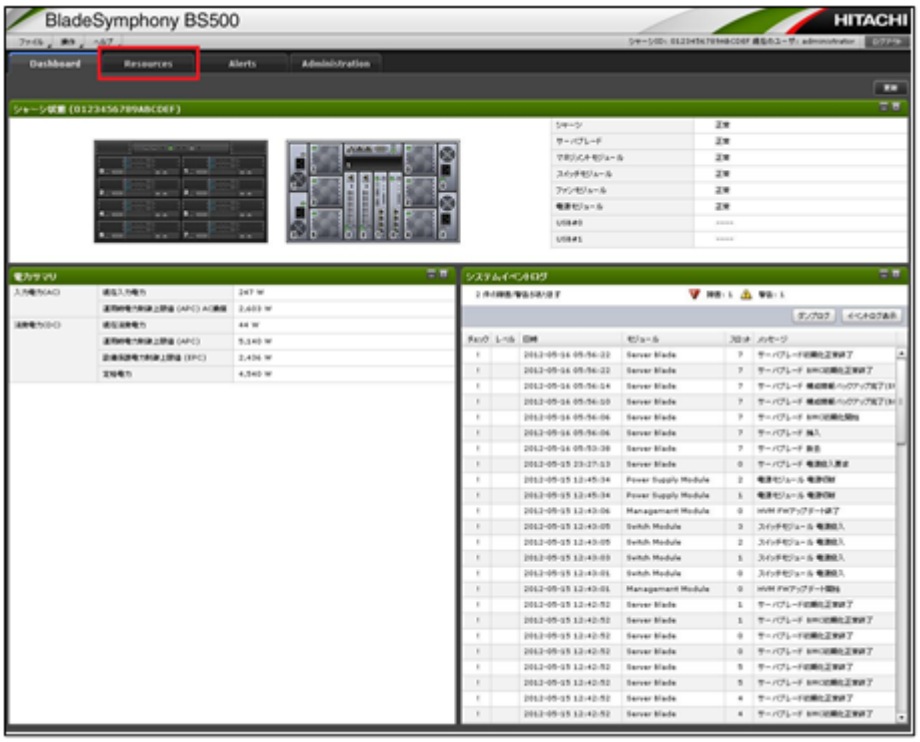
本現象が発生した場合は，[更新]ボタンのクリックにより，画面を更新してください。

2.19.6 LPAR 作成

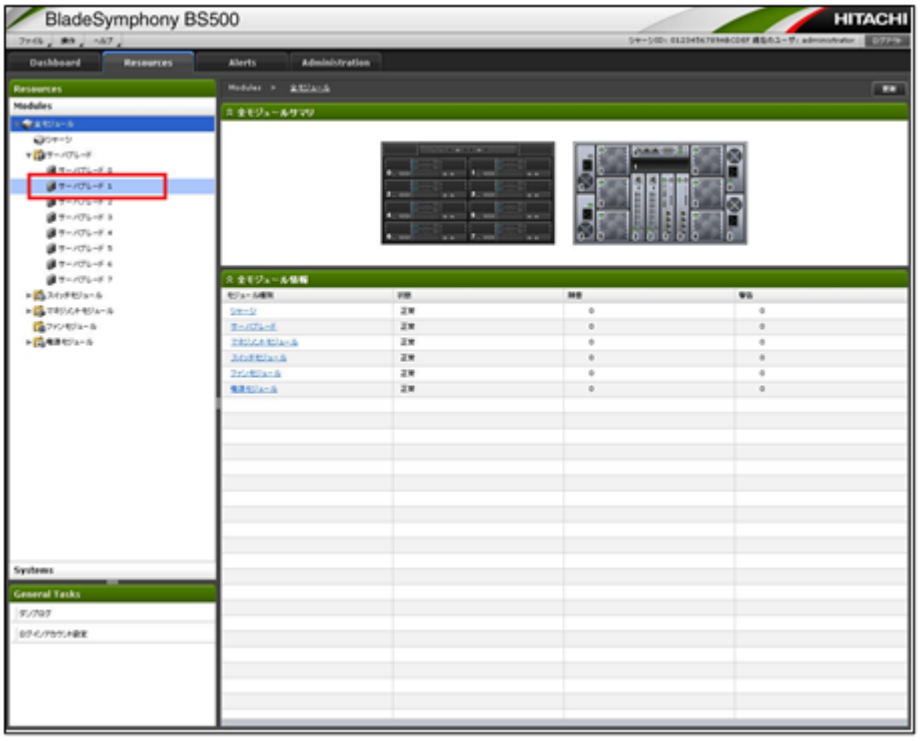
LPAR を作成する手順を説明します。

なお，動作モードが HVM でサーバブレードの電源が ON の場合に，LPAR を作成することができます。

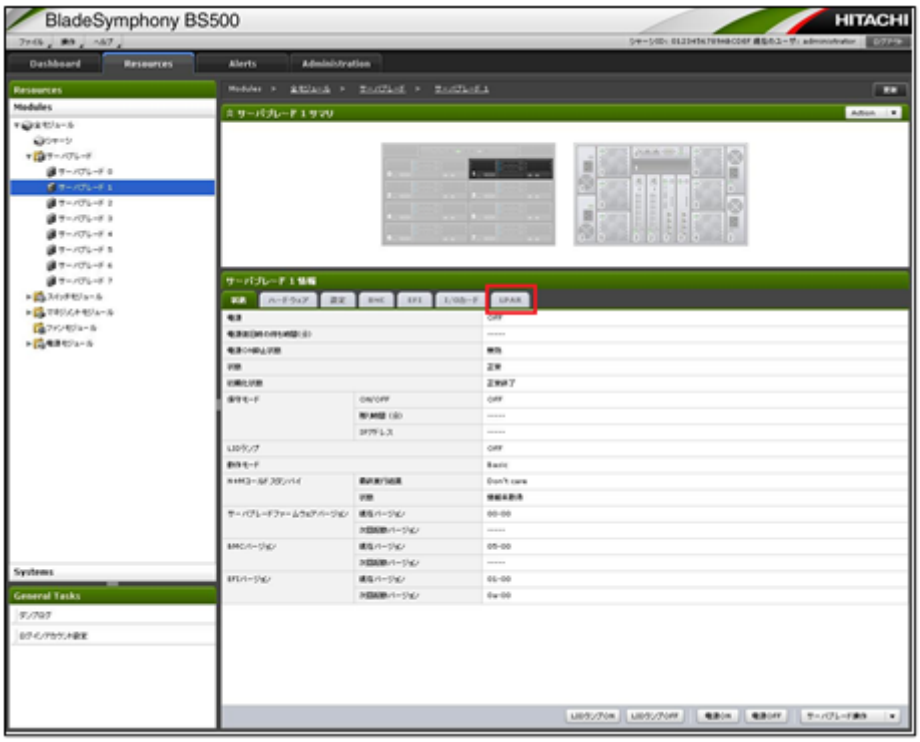
1. [Resources]タブをクリックします。



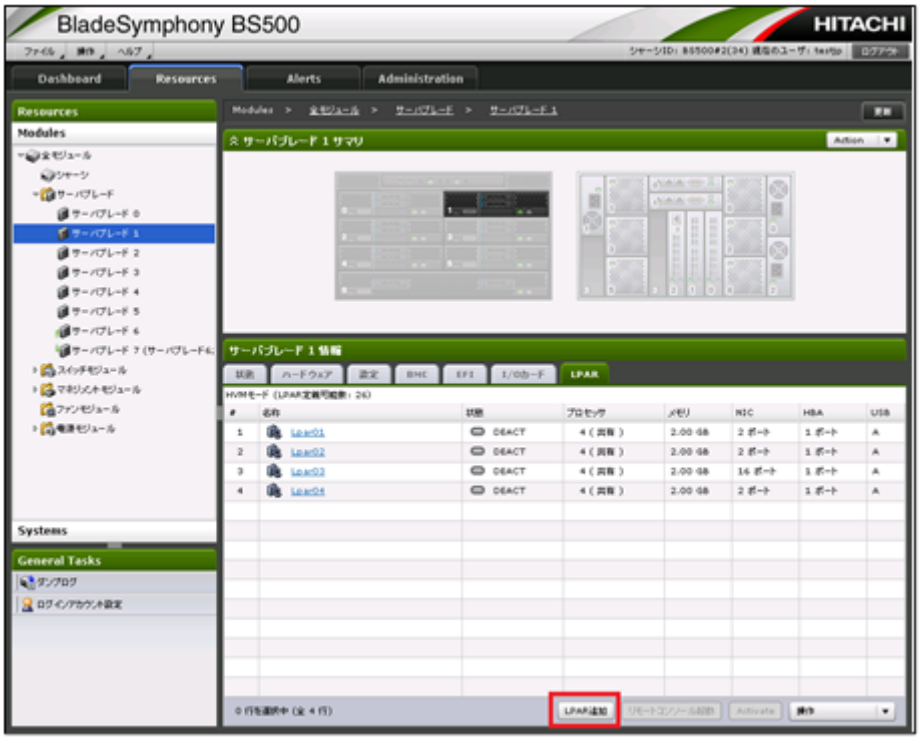
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。

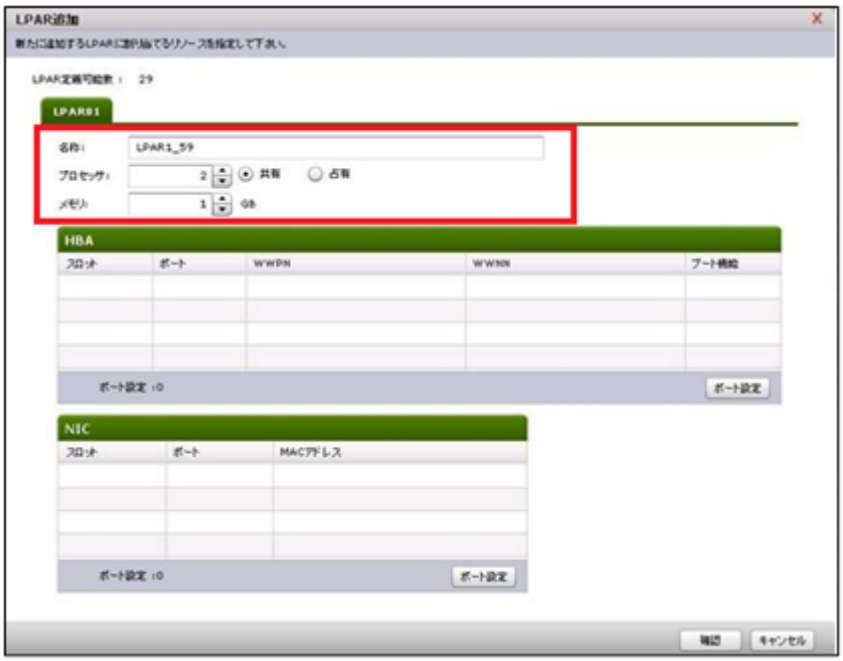


4. [LPAR 追加]ボタンをクリックします。



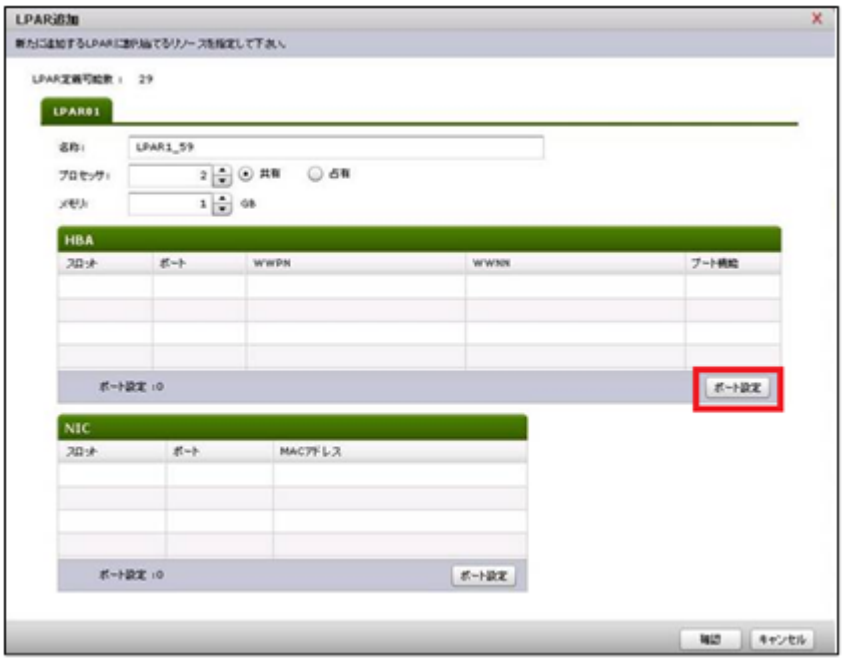
5. LPAR 名称，割り当てプロセッサ数，プロセッサのスケジューリングモード，および割り当てメモリ容量を設定します。

   なお，割り当て可能なプロセッサ数の上限は 64 で，割り当て可能なメモリ容量の上限は（搭載メモリ容量－HVM が使用するメモリ容量）GB です。



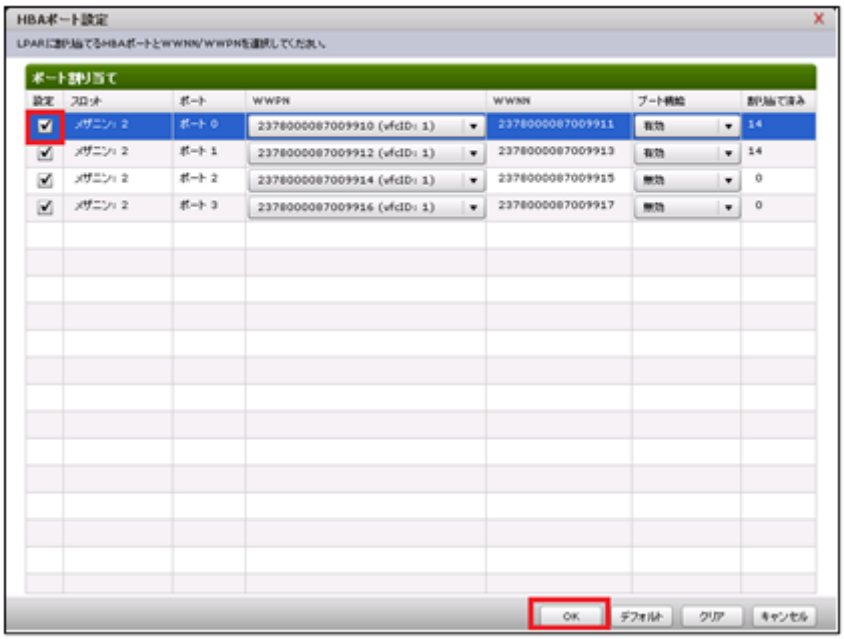
参考 LPAR 名称は，デフォルトで"LPARX_xx"(X:LPAR 番号, xx:HVM に割り当てられた VNIC System Number)と設定されています。

6. [HBA]パネルの[ポート設定]ボタンをクリックします。

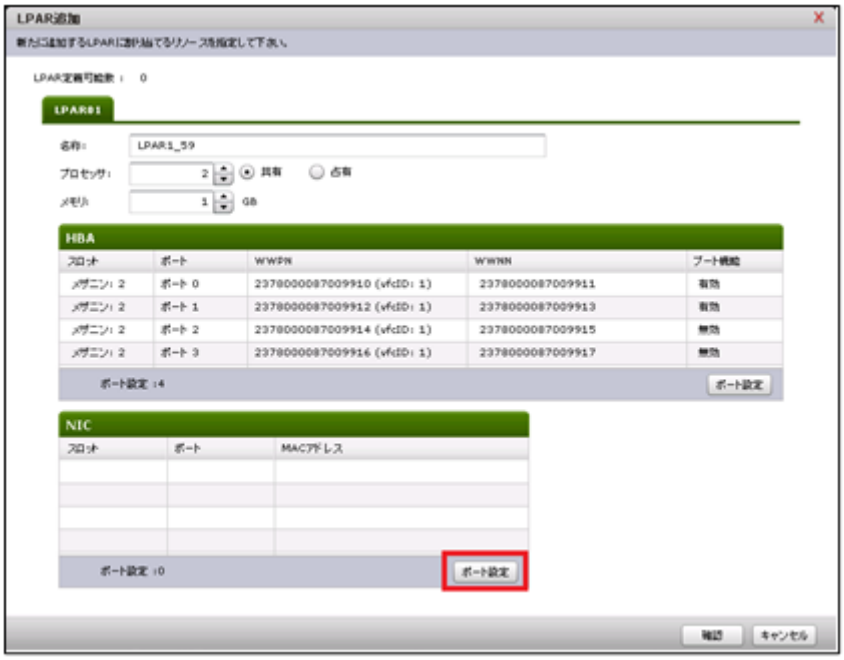


7. 割り当てるポートの設定列のチェックボックスにチェックをつけ，[OK]ボタンをクリックします。

   なお，割り当て可能なポートの上限は，搭載されているポート数となります。

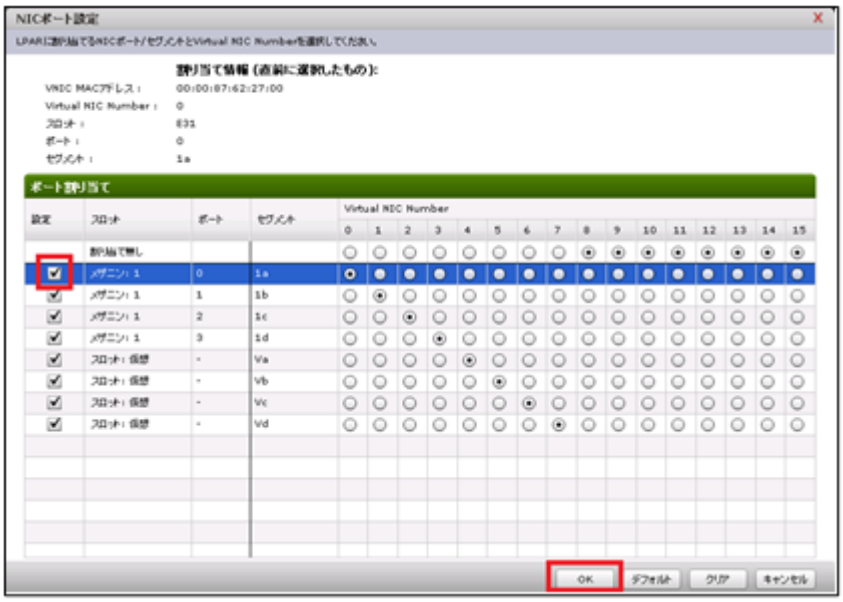


8. [NIC]パネルの[ポート設定]ボタンをクリックします。



9. 割り当てるポートの設定行のチェックボックスにチェックをつけ，[OK]ボタンをクリックします。

   なお，割り当て可能なポート（セグメント）の上限は，共有 NIC（1a，1b，･･･）が 16，仮想 NIC（Va，Vb，･･･）が 4 となります。



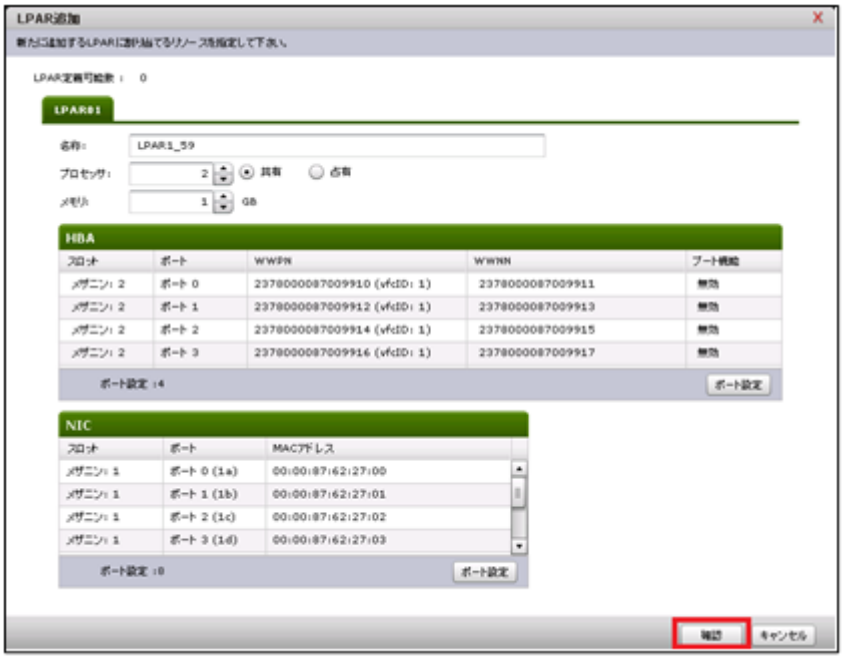
マネジメントモジュールファームウェアバージョンが A0200 以前の場合は，手順 13 に進んでください。

マネジメントモジュールファームウェアバージョンが A0205 以降の場合は，手順 10 に進んでください。

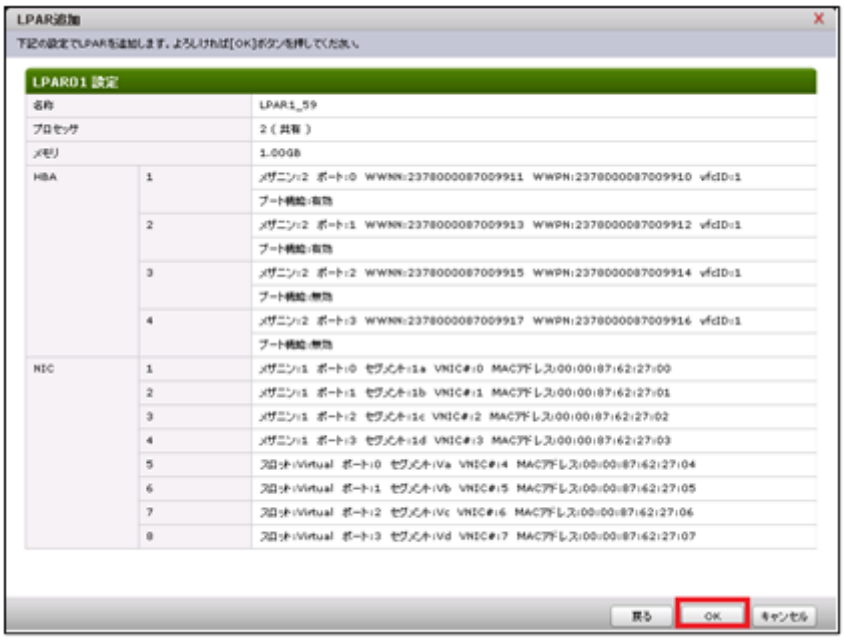
10. LPAR 追加ダイアログで[USB]パネルの[ポート設定]ボタンをクリックします。
11. USB ポート設定ダイアログが表示されます。

    割り当てるポートの設定列のチェックボックスにチェックをつけ，[OK]ボタンをクリックします。

    なお，割り当て可能なポートの上限は，搭載されているポート数となります。
12. Boot Mode を変更する場合，Advanced Option エリアの Boot Mode プルダウンリストから使用するモードを選択します。
13. [確認]ボタンをクリックします。



14. [OK]ボタンをクリックします。

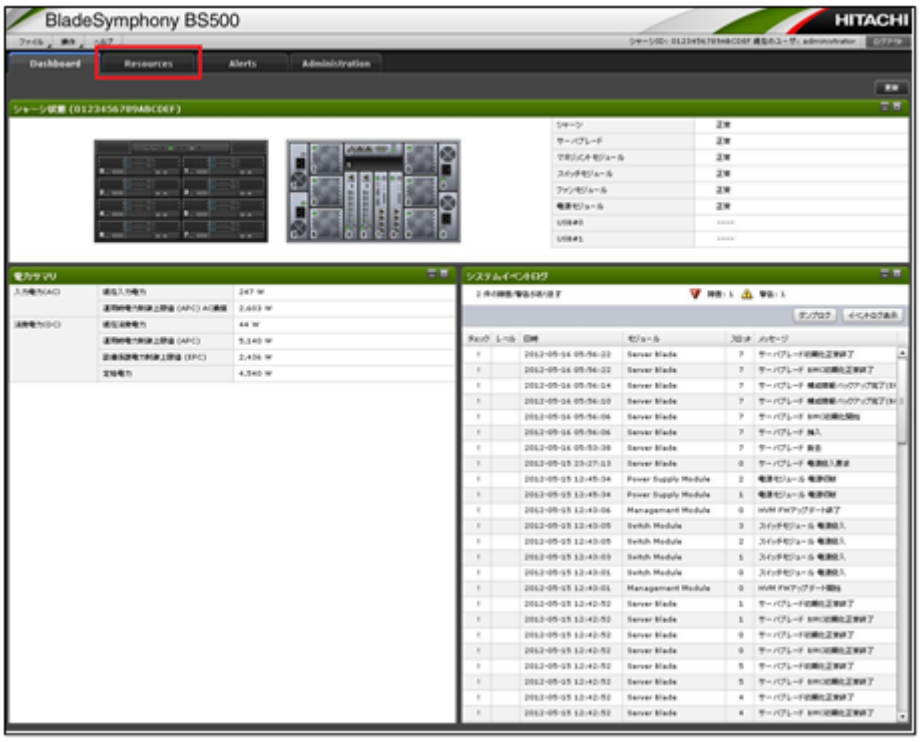


2.19.7 HVM 構成情報の保存

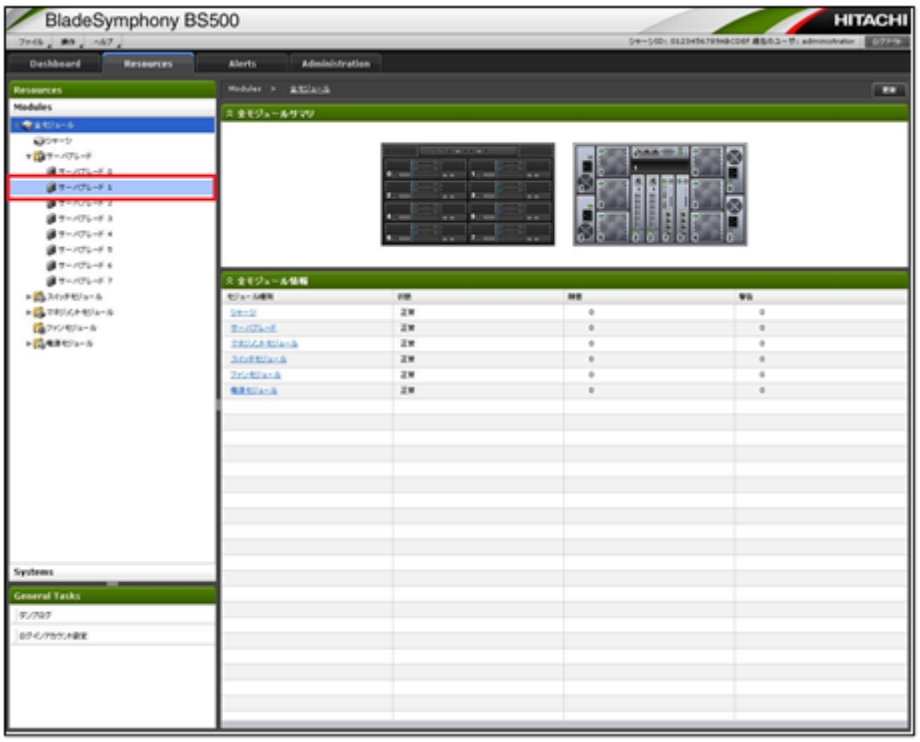
HVM 構成情報を保存する手順を説明します。

なお，サーバブレードが電源 ON の場合に，HVM 構成情報を保存することができます。

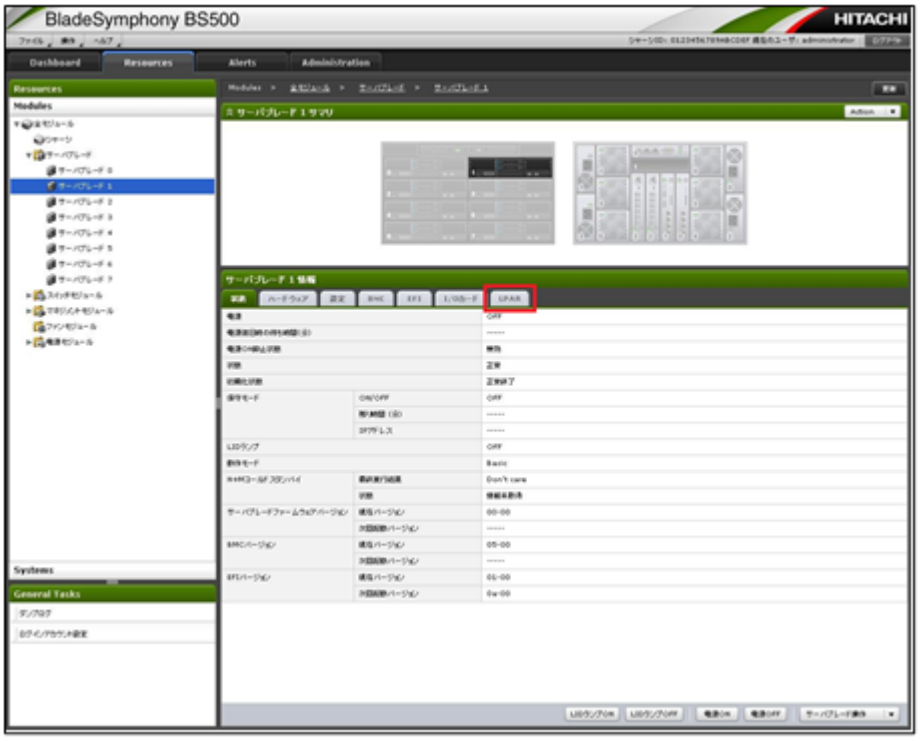
1. [Resources]タブをクリックします。



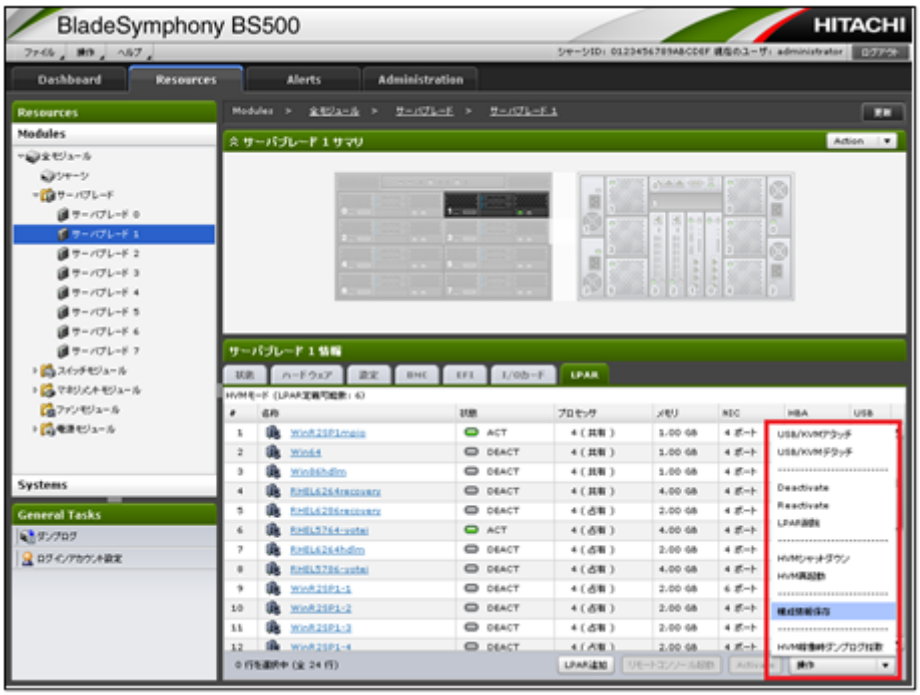
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブにある[操作]メニュー内の[構成情報保存]をクリックします。



5. [OK]ボタンをクリックします。

6. [閉じる]ボタンをクリックします。

2.19.8 LPAR への USB 割り当ての設定

【マネジメントモジュールファームウェアバージョン A0205 以降】

LPAR に USB を割り当てる手順を説明します。なお，LPAR の状態が DEACT の場合に，USB 割り当てを設定，変更することができます。

1. Web コンソールで[Resources]タブをクリックします。
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。
3. [サーバブレード n]パネルの[LPAR]タブを選択します。

4. USB デバイスを割り当てる LPAR を選択し，[Action]メニューから[Edit USB Assign]を選択します。
5. [USB ポート設定]ダイアログが表示されます。

   LPAR に割り当てるポートを選択し，[OK]ボタンをクリックします。なお，複数の USB ポートがある場合，リモートコンソール呼び出しに使用するポートは"USB/KVM"と表示されます。
6. [USB ポート設定]の確認ダイアログが表示されます。内容を確認し，[OK]ボタンをクリックします。

2.19.9 LPAR のブートオーダ設定

【マネジメントモジュールファームウェアバージョン A0125 以降】

LPAR 上でゲスト OS をセットアップするためのブートオーダを設定する手順を説明します。

なお，LPAR の状態が DEACT の場合に，ブートオーダを設定，変更することができます。

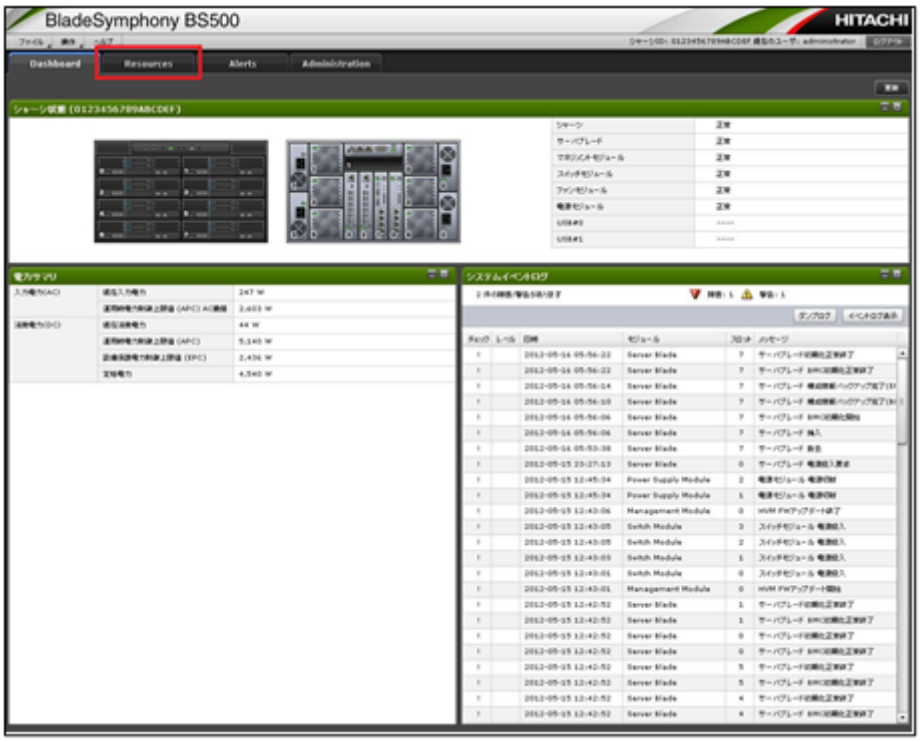
本操作が可能なサーバブレードと HVM ファームウェアバージョンの組み合わせを次に示します。

サーバブレード	HVM ファームウェアバージョン
BS520H サーバブレード A1/B1	01-0X～
BS520H サーバブレード A2/B2	01-6X～
BS520H サーバブレード B3	02-05～
BS520A サーバブレード A1	01-1X～
BS540A サーバブレード A1/B1	01-2X～
BS520X サーバブレード B1	02-02～
BS520X サーバブレード B2	02-2X～

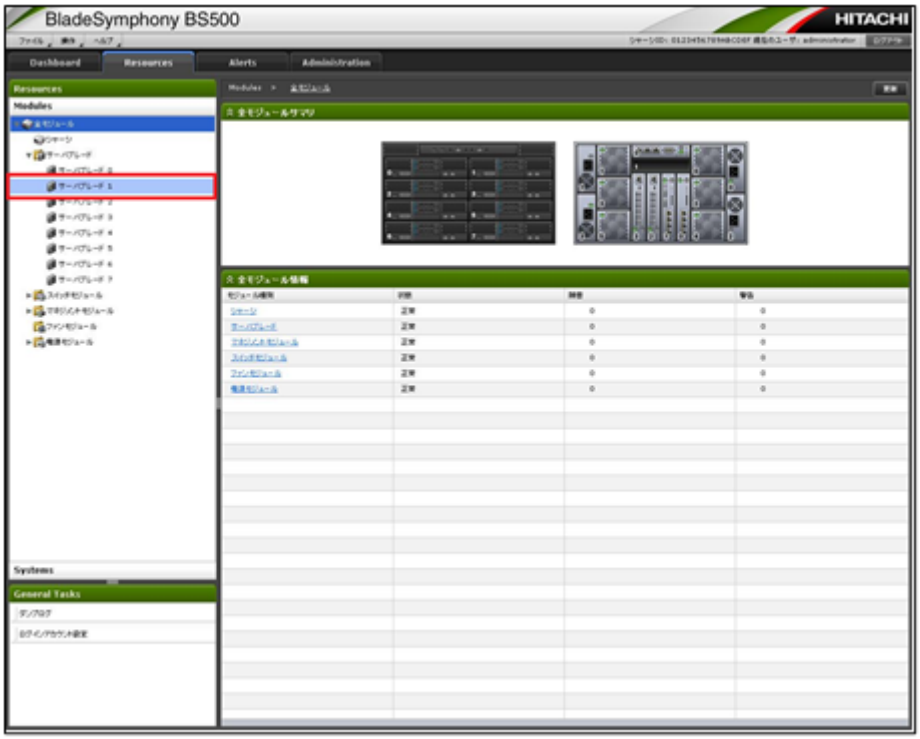
マネジメントモジュールファームウェアバージョン A0120 以前では，本操作ができません。LPAR のブートオーダ設定については，「*BladeSymphony BS500 HVM ユーザーズガイド*」を参照してください。

(1) ブートオーダの設定

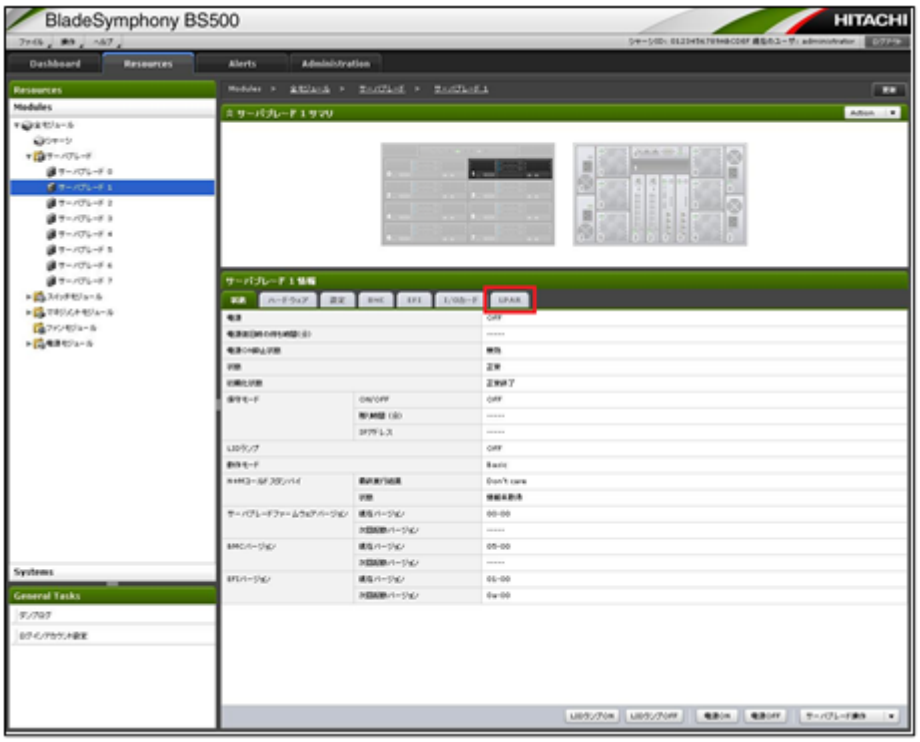
1. [Resources]タブをクリックします。



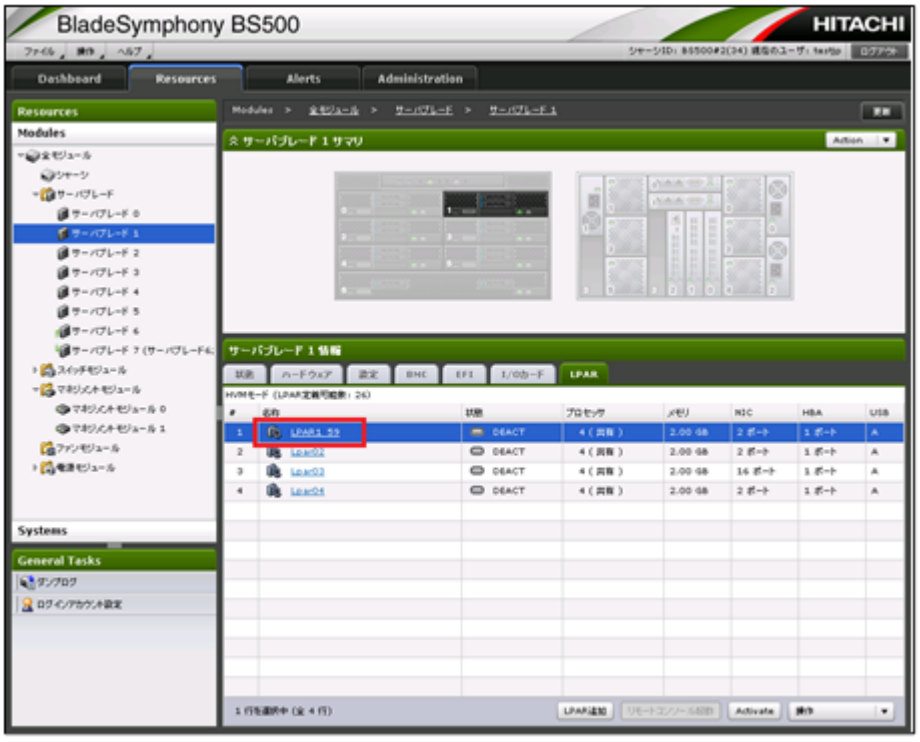
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



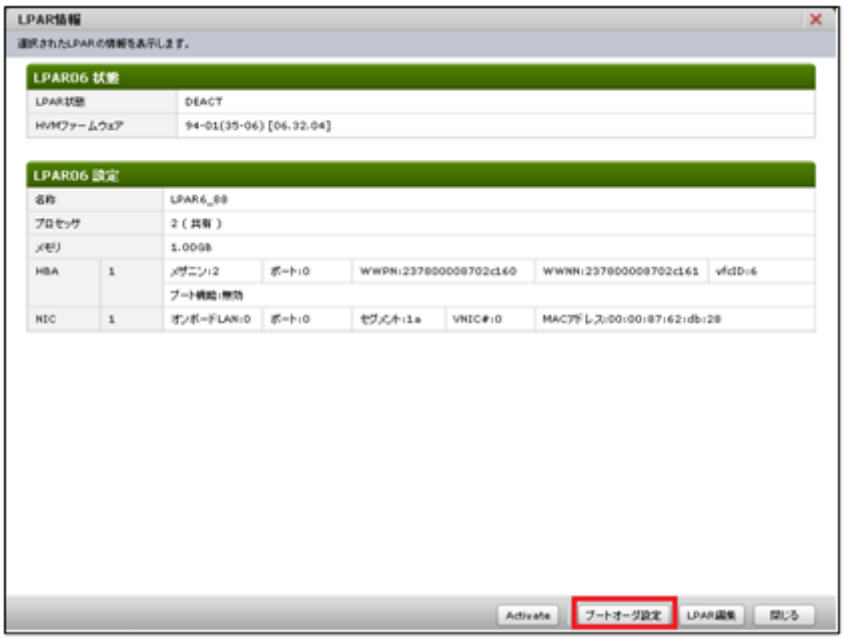
3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブでブート設定を行う LPAR を選択し，LPAR 名称をクリックします。

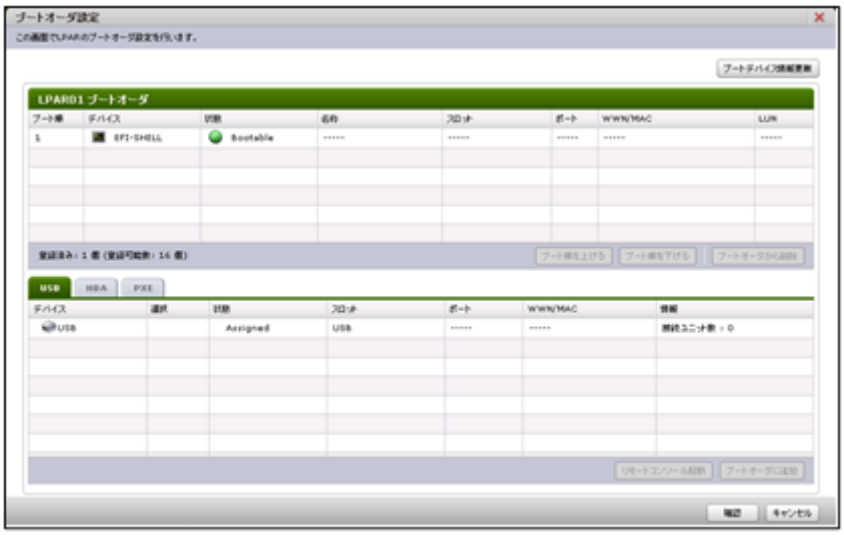


5. LPAR の設定内容を確認し，[ブートオーダ設定]ボタンをクリックします。



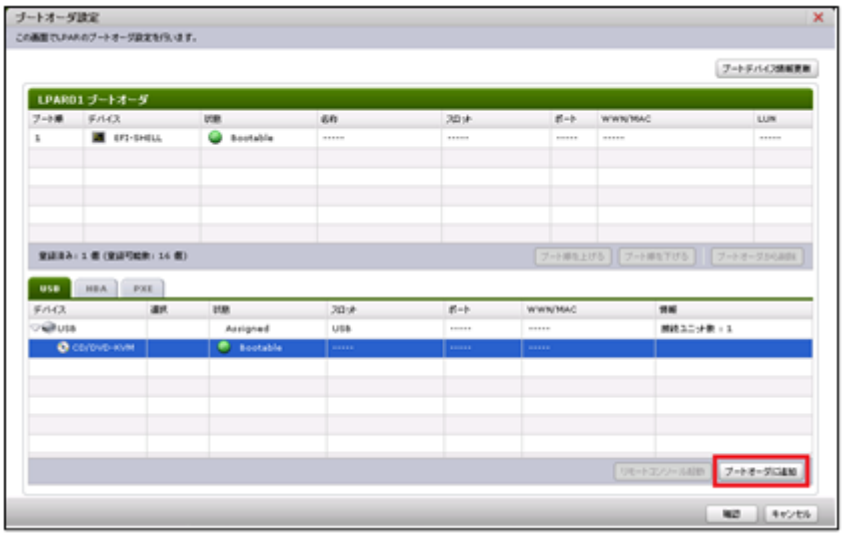
6. [OK]ボタンをクリックします。

7. [ブートオーダ設定]画面が表示されます。



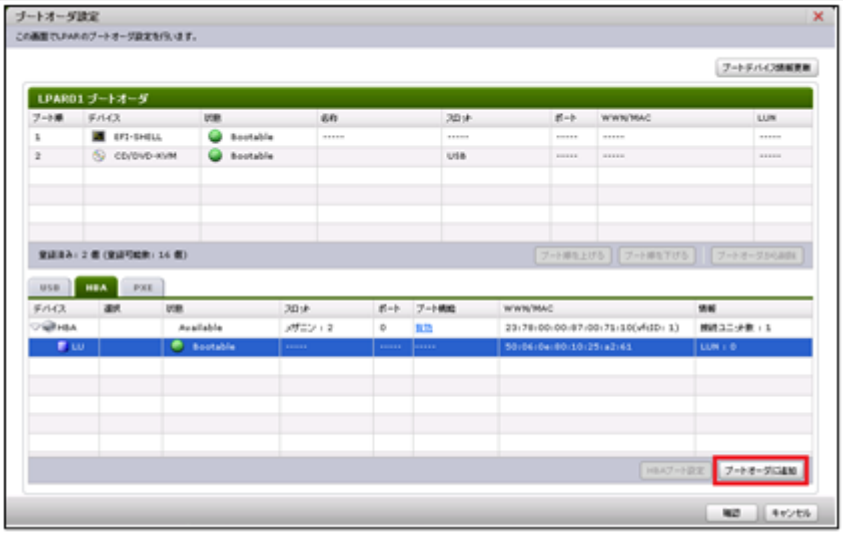
8. [USB]タブで追加するデバイスを選択し，[ブートオーダに追加]ボタンをクリックします。
   必要なデバイスが表示されていない場合，「(2) 仮想ドライブの接続」の手順に従って，デバイスを認識させてください。

参考 【マネジメントモジュールファームウェアバージョン A0205 以降】
LPAR に複合 USB ポートが割り当てられている場合，単一のポートが表示されます。



9. [HBA]タブで追加するデバイスを選択し，[ブートオーダに追加]ボタンをクリックします。
   必要なデバイスが表示されていない場合，「(3) HBA ブートドライバの設定」の手順に従って設定を行い，デバイスを認識させてください。

参考 ブートモードが UEFI Mode の場合は，OS インストールを行うことにより，HBA デバイスが自動的にブートオーダに追加されるため，HBA デバイスを追加する必要はありません。

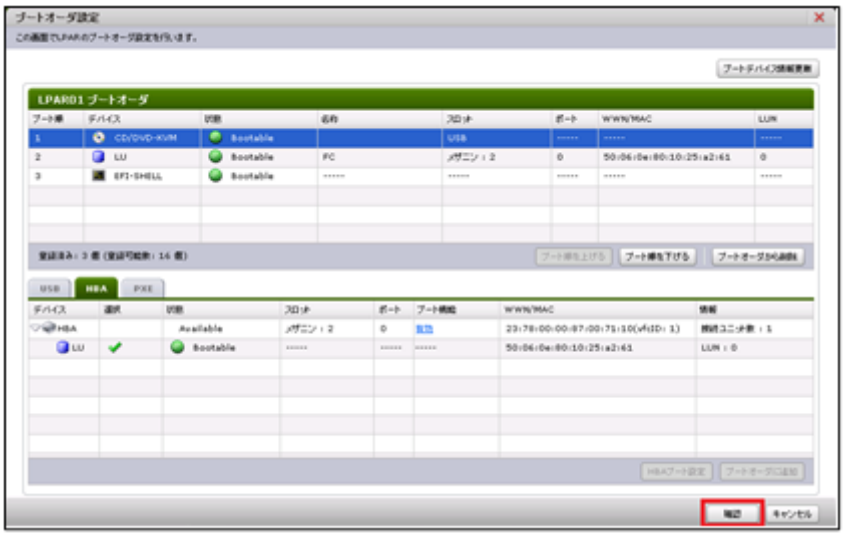


10. [ブート順を上げる][ブート順を下げる]ボタンを用いて，次のようにブートオーダを変更し，[確認]ボタンをクリックします。
    ブートモードが Legacy Mode の場合は，

    - LU
    - CD/DVD-KVM
    - EFI-SHELL

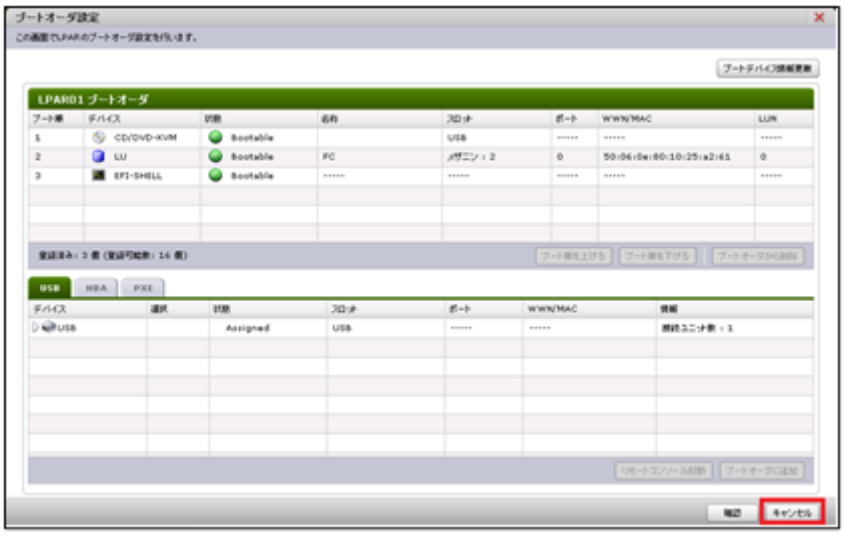
    ブートモードが UEFI Mode の場合は，

    - CD/DVD-KVM
    - EFI-SHELL

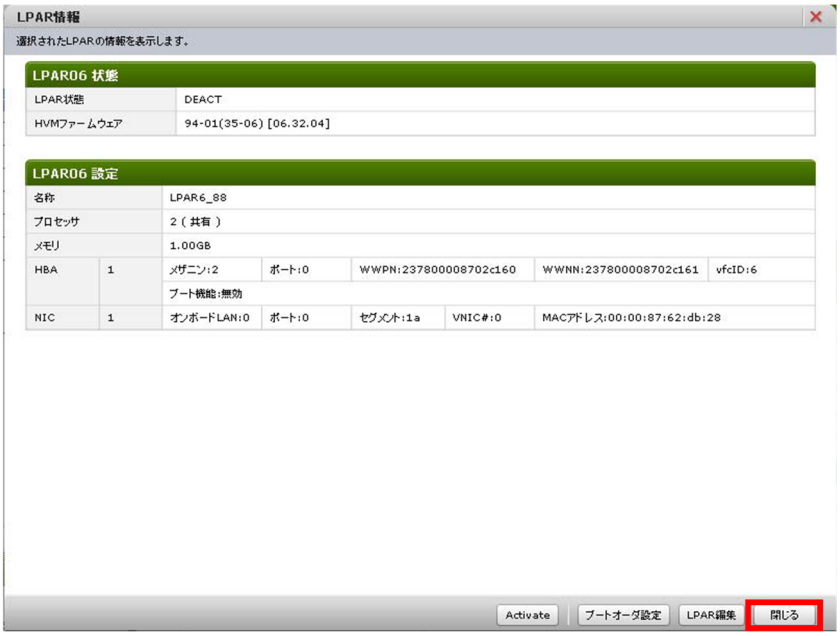


11. [OK]ボタンをクリックします。

12. [キャンセル]ボタンをクリックします。



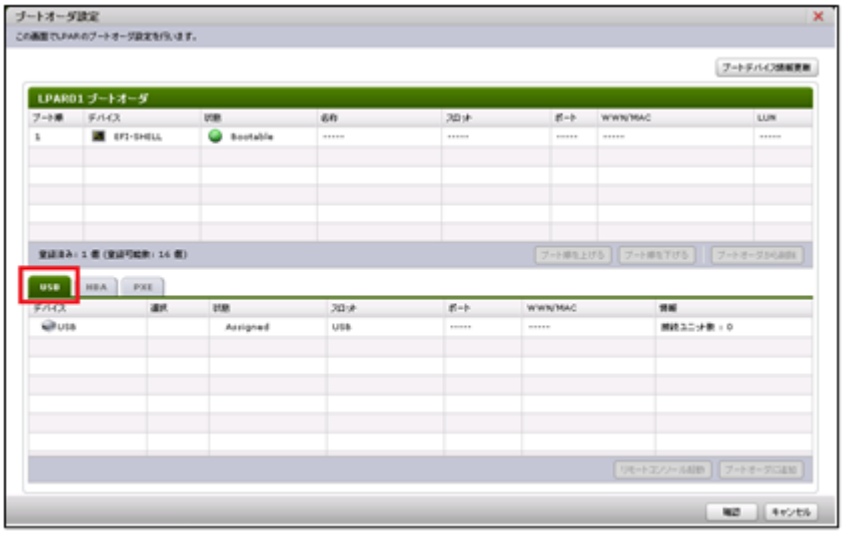
13. [閉じる]ボタンをクリックします。



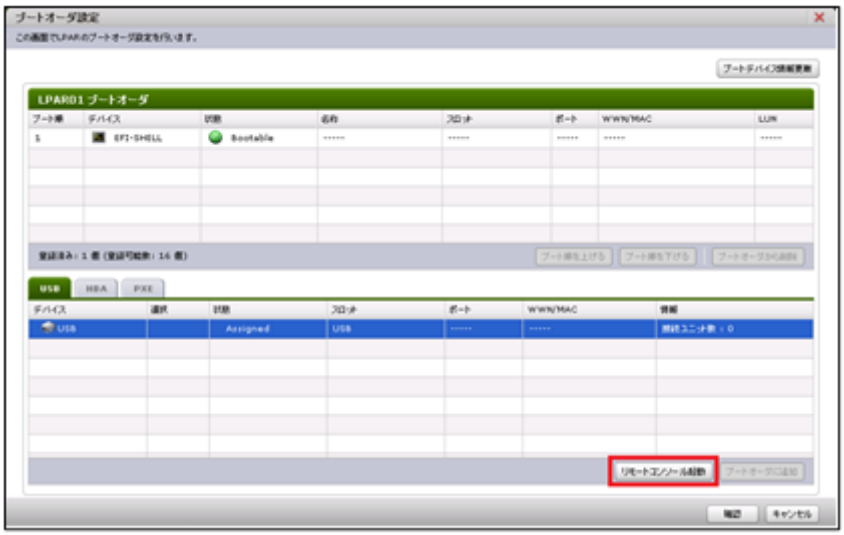
(2) 仮想ドライブの接続

[USB]タブに必要なデバイスが表示されていない場合，リモートコンソールの仮想メディア機能を用いてデバイスを接続する必要があります。次の手順にしたがって仮想ドライブを接続し，デバイスとして認識させてください。

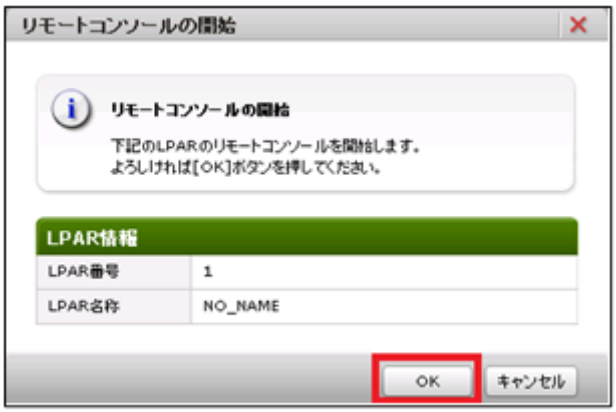
1. [ブートオーダ設定]画面で[USB]タブを選択します。



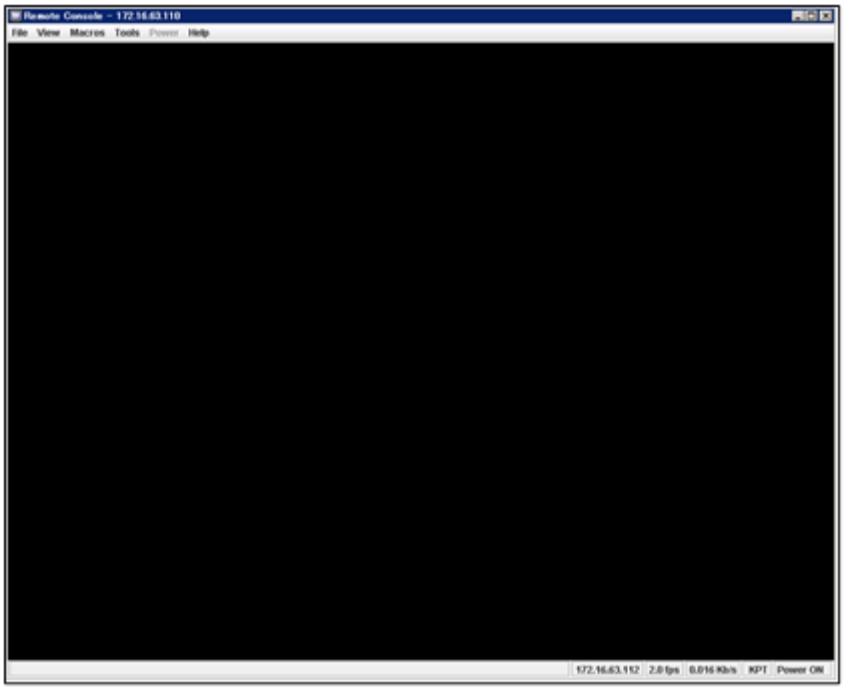
2. USB デバイスを選択し，[リモートコンソール起動]ボタンをクリックします。



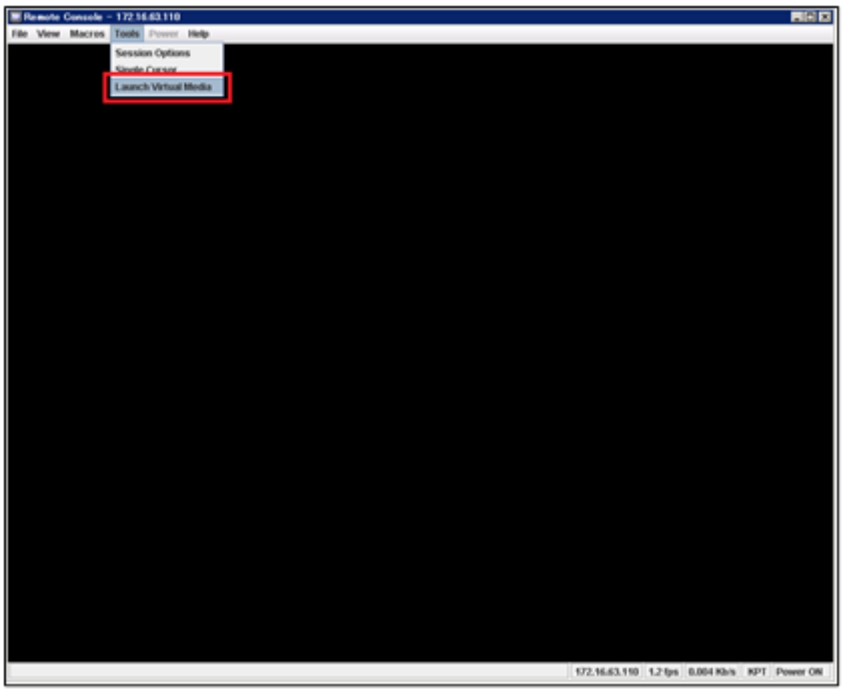
3. [OK]ボタンをクリックします。



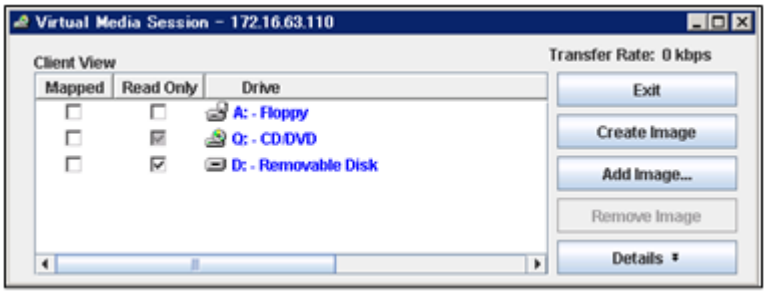
4. リモートコンソールが表示されます。



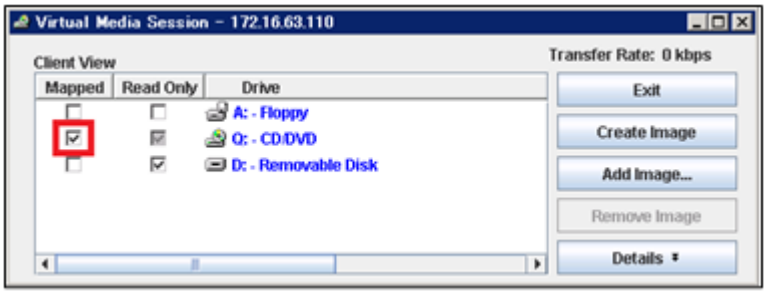
5. リモートコンソールのメニューの[Tools] - [Launch Virtual Media］をクリックします。



6. 仮想メディアコンソール画面が表示されます。



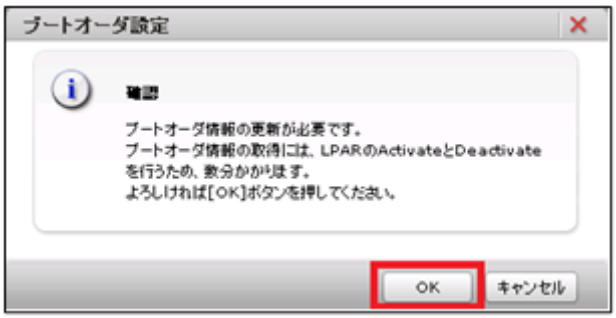
7. ブートデバイスとして使用する CD/DVD ドライブ，またはイメージファイルの Mapped にチェックをつけます。



重要 仮想ドライブを使用している間は，仮想メディアコンソールの[Exit]ボタンや[x]ボタンなどで画面を閉じないでください。また，リモートコンソールも終了させないでください。仮想メディアコンソール画面またはリモートコンソールを閉じると，仮想メディアセッションが終了し，すべてのドライブをサーバブレードから切り離してしまうため，ドライブが認識されなくなります。

参考 リモートコンソール，および仮想メディアコンソールについての詳細は，「*BladeSymphony BS500 リモートコンソールユーザーズガイド*」を参照してください。

8. ブートオーダ設定画面に次のメッセージが表示されていることを確認し，[OK]をクリックします。

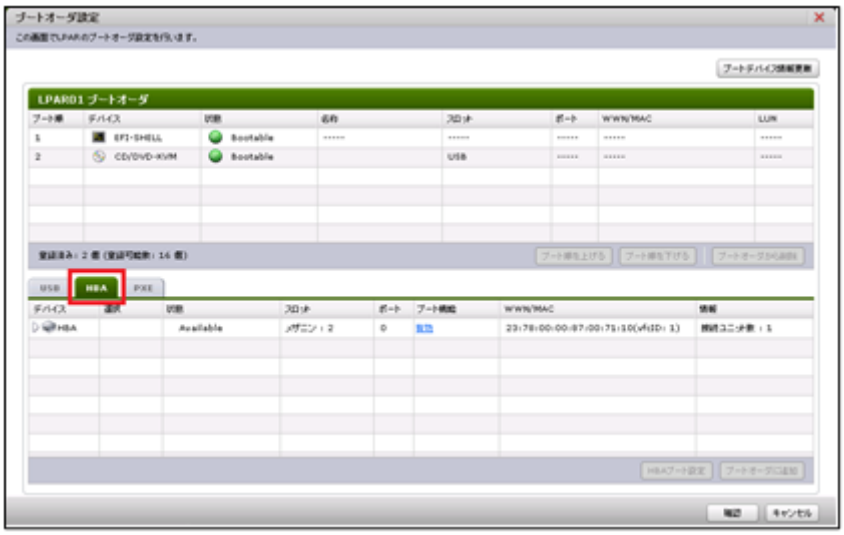


9. USB デバイスに仮想ドライブがブートデバイスとして追加されます。

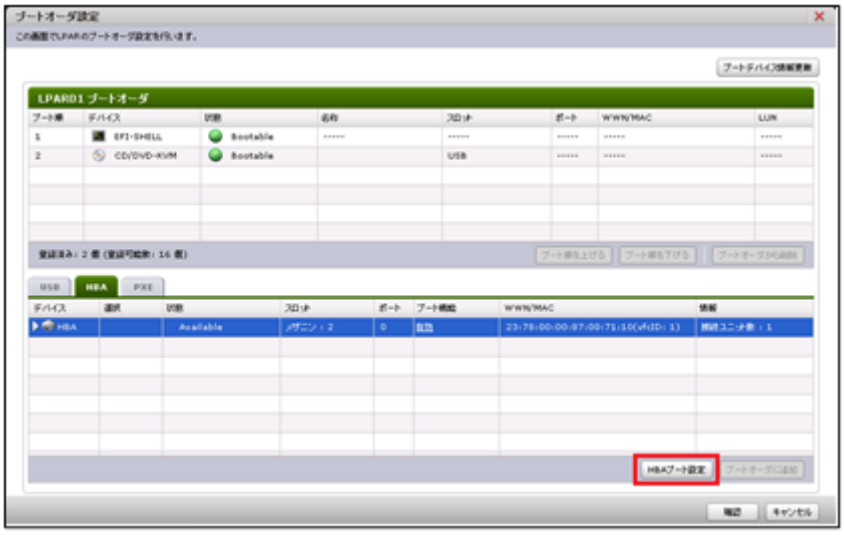
(3) HBA ブートドライバの設定

[HBA]タブに必要なデバイスが表示されていない場合，次の手順に従って HBA ブートドライバの設定を確認し，必要な設定を行ってください。

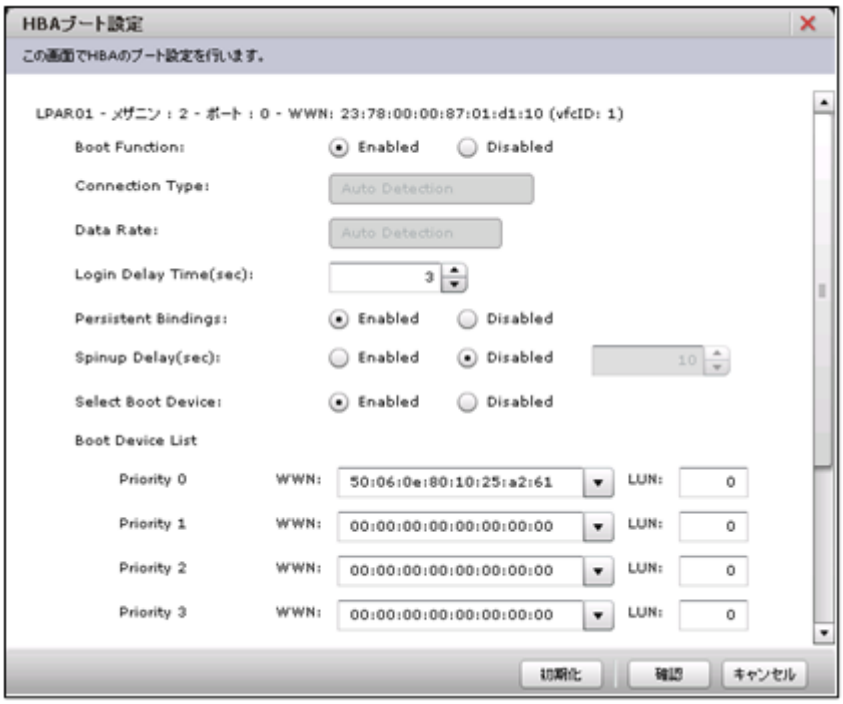
1. [ブートオーダ設定]画面で[HBA]タブを選択します。



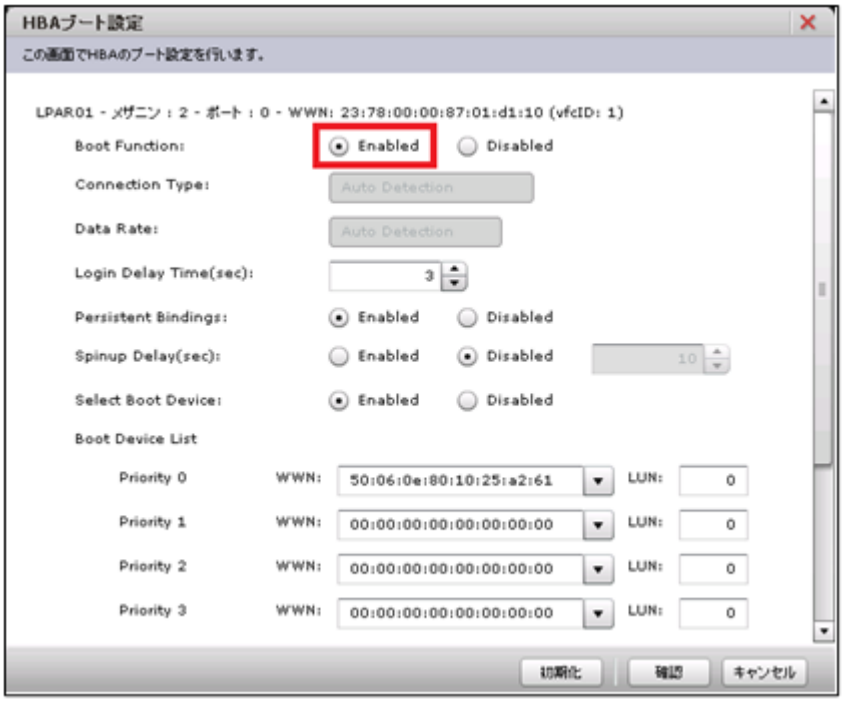
2. HBA ポートを選択し，[HBA ブート設定]ボタンをクリックします。



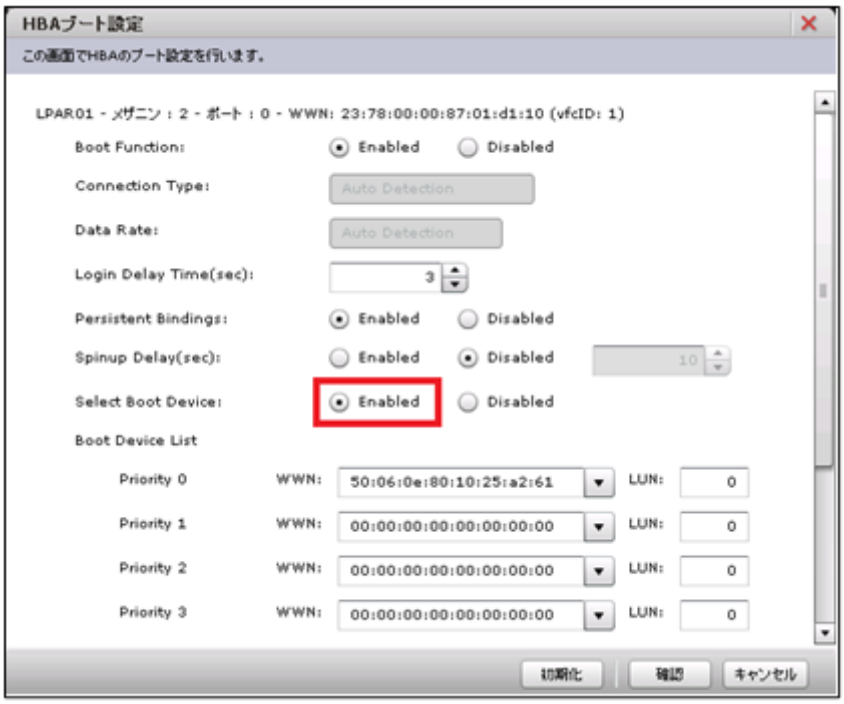
3. [HBA ブート設定]画面が表示されます。



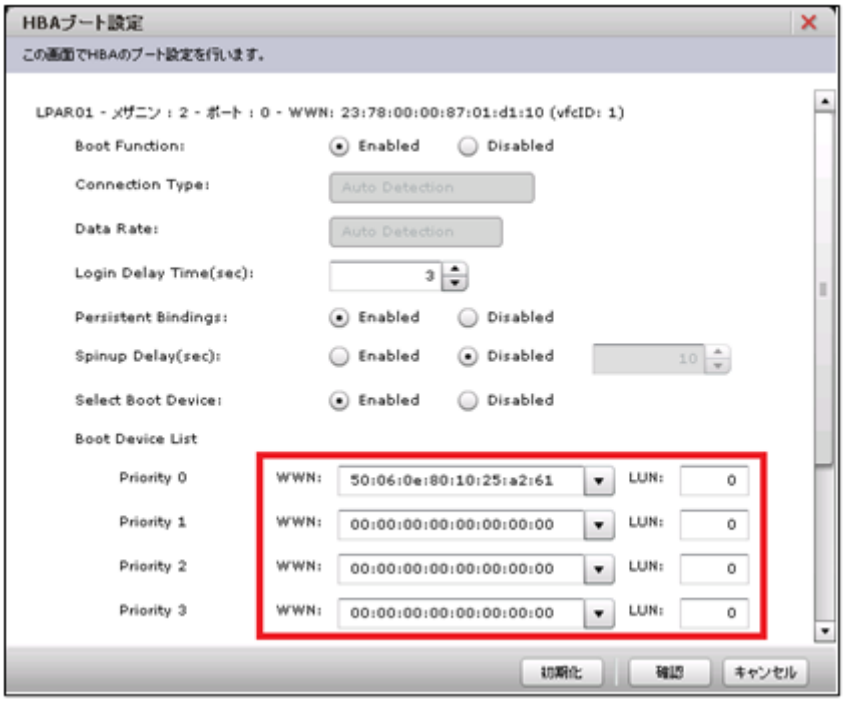
4. [Boot Function]で[Enable]ラジオボタンを選択します。



5. [Select Boot Device]で[Enable]ラジオボタンを選択します。

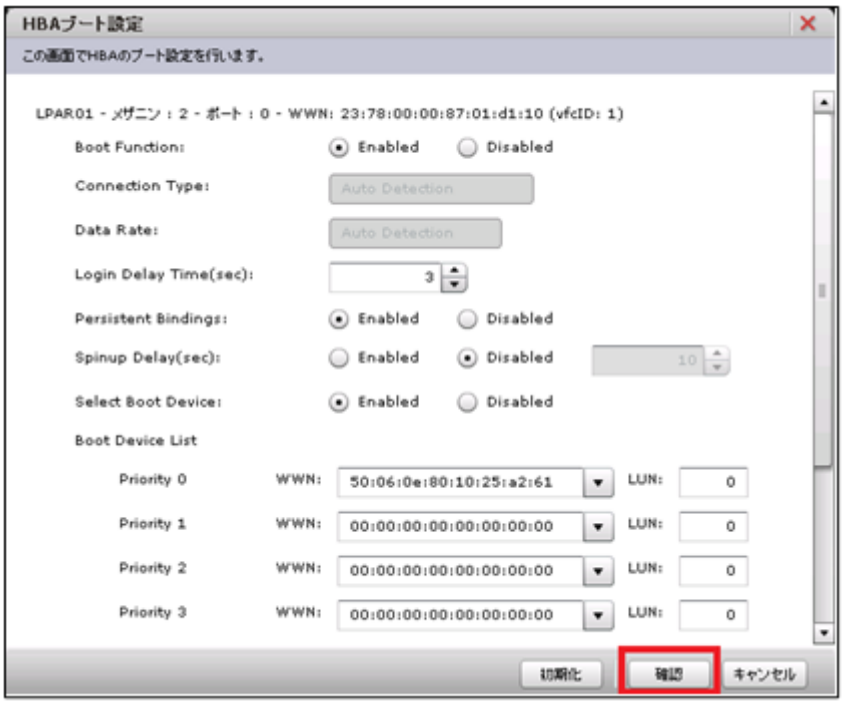


6. [Boot Device List]の[WWN]コンボボックスに接続対象となる外付けディスクアレイ装置のポートの WWN を，[LUN]テキストボックスに接続対象となる外付けディスクアレイ装置のポートの LU 番号を設定します。

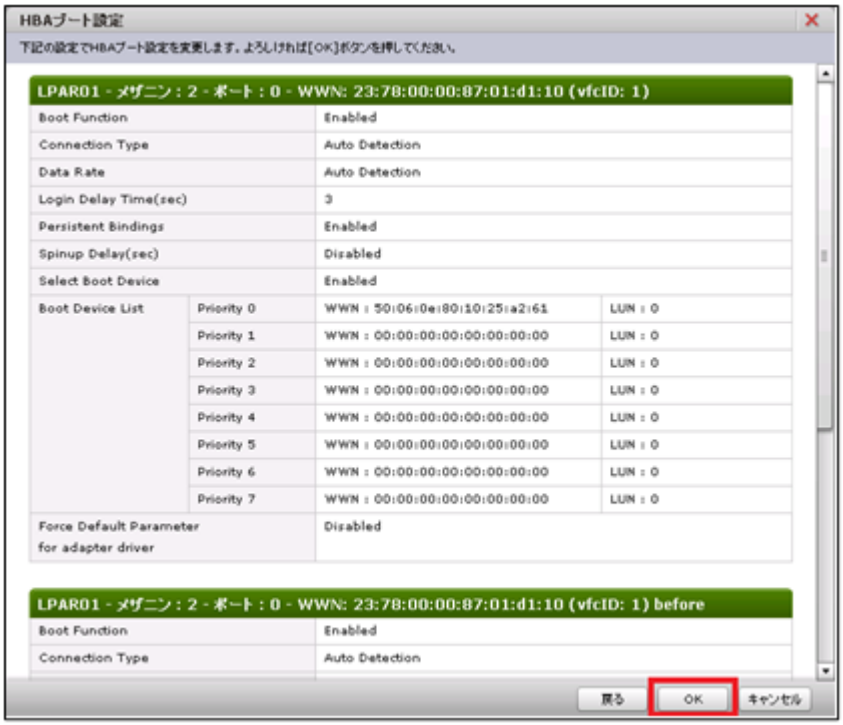


参考 設定についての詳細は，「*HITACHI Gigabit Fibre Channel アダプタユーザーズガイド(BIOS/EFI 編)*」を参照してください。

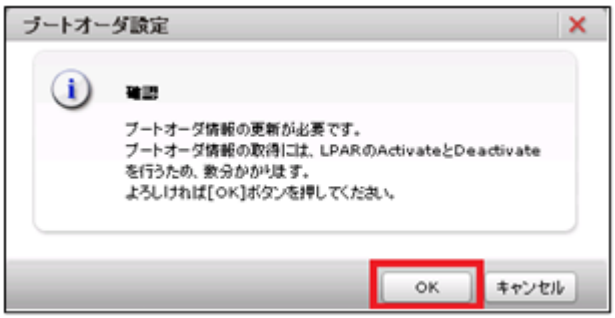
7. [確認]ボタンをクリックします。



8. [OK]ボタンをクリックします。



9. [OK]ボタンをクリックします。

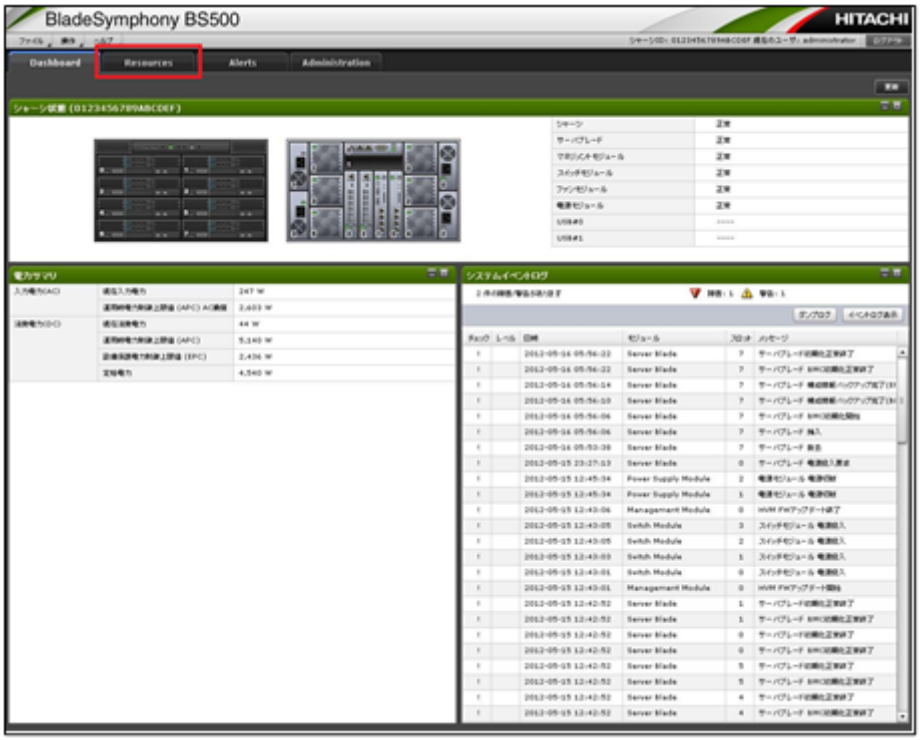


10. HBA ポートにデバイスが追加されます。

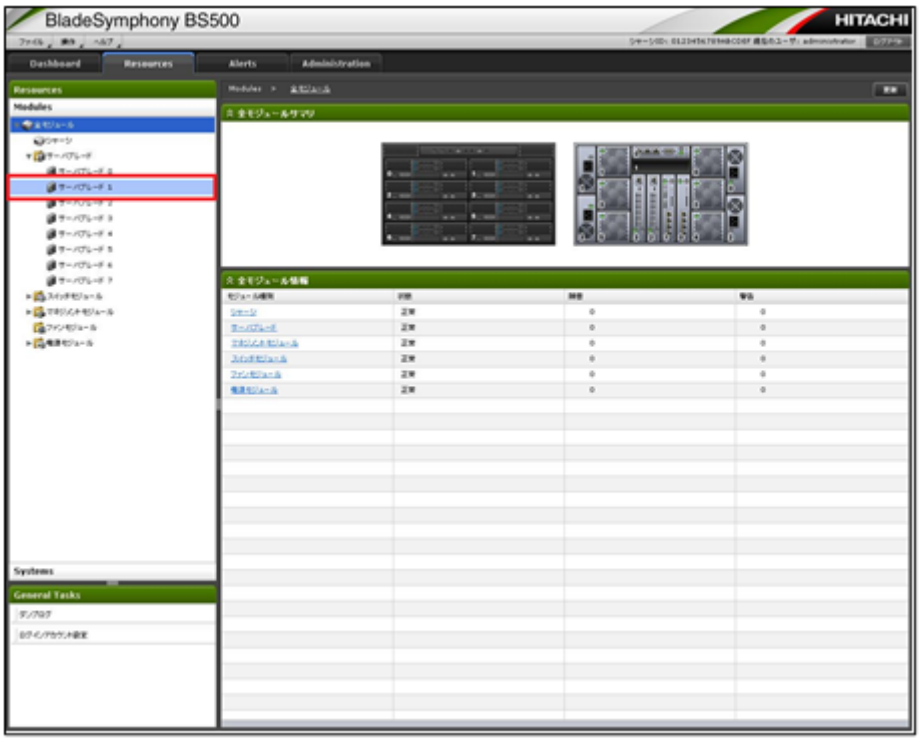
2.19.10 LPAR の Activate

LPAR を Activate する手順を説明します。

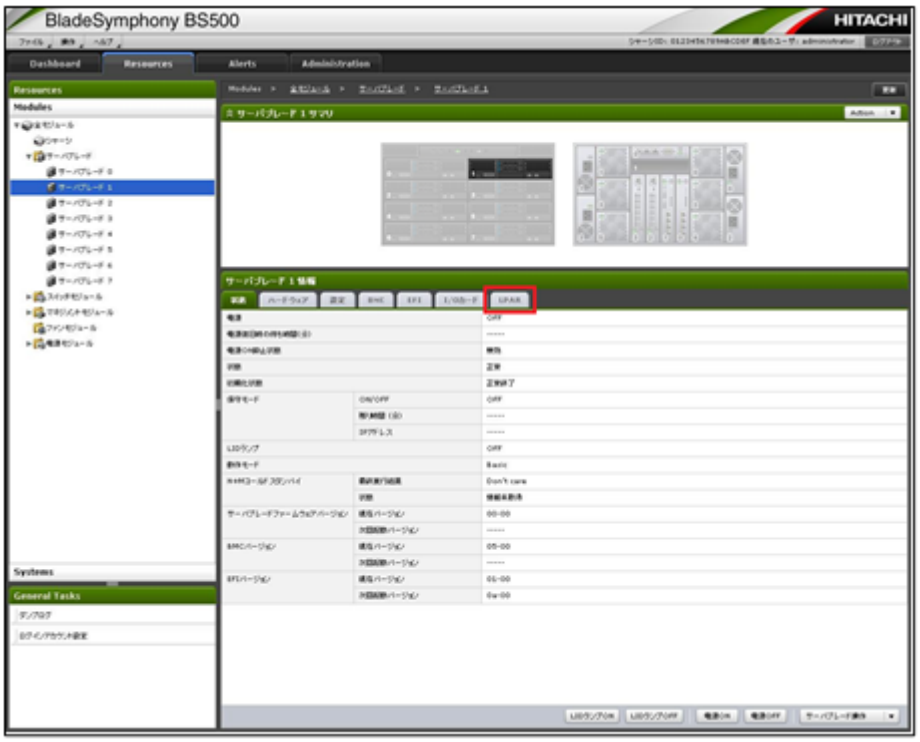
1. [Resources]タブをクリックします。



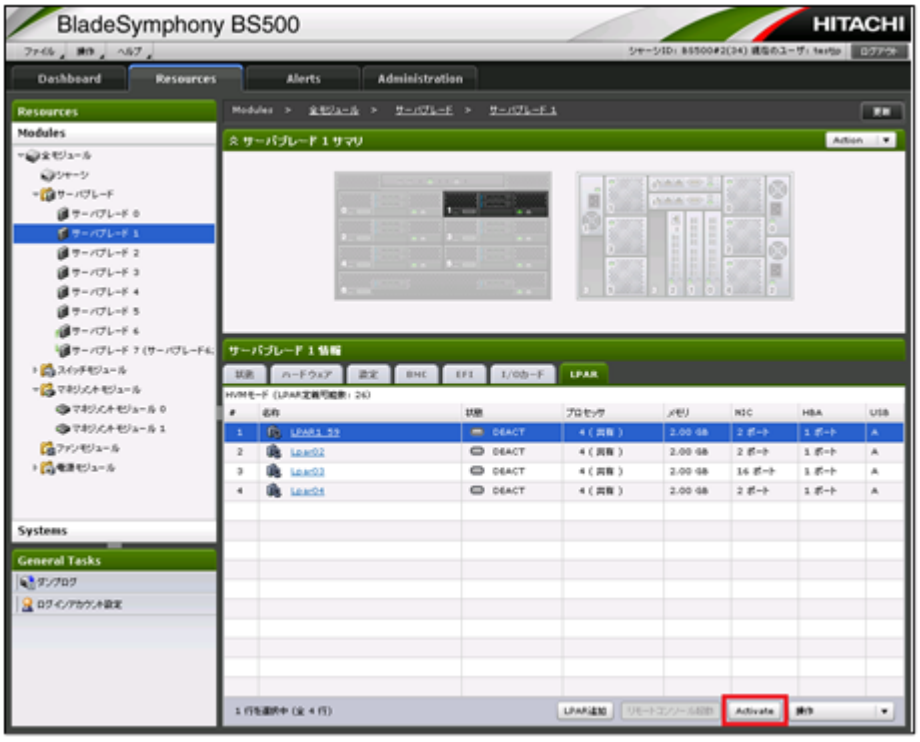
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブで Activate する LPAR を選択し，[Activate]ボタンをクリックします。

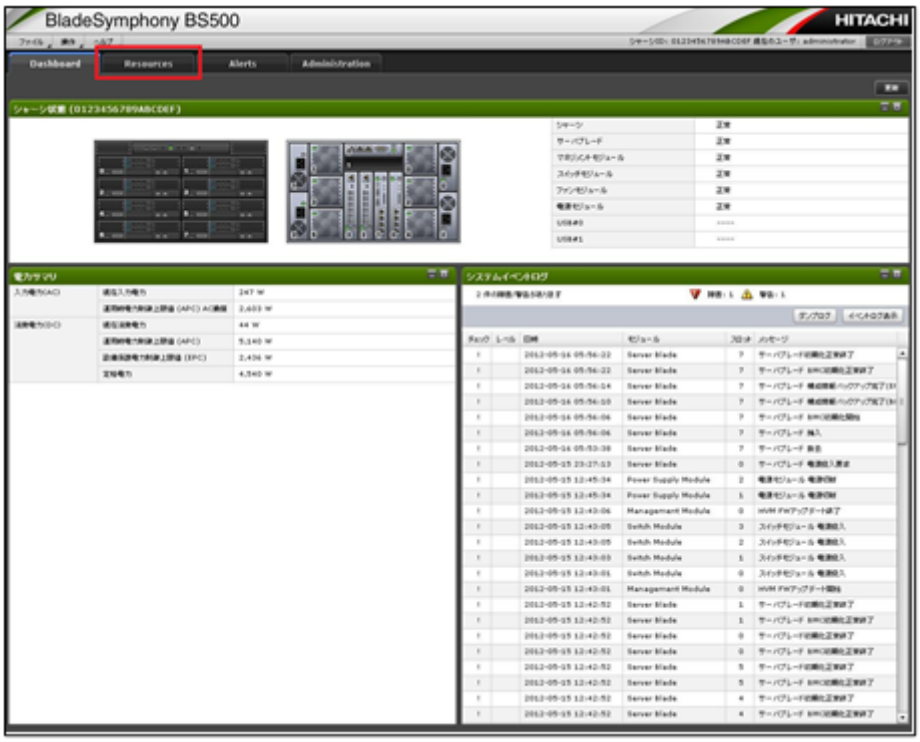


5. [OK]ボタンをクリックします。

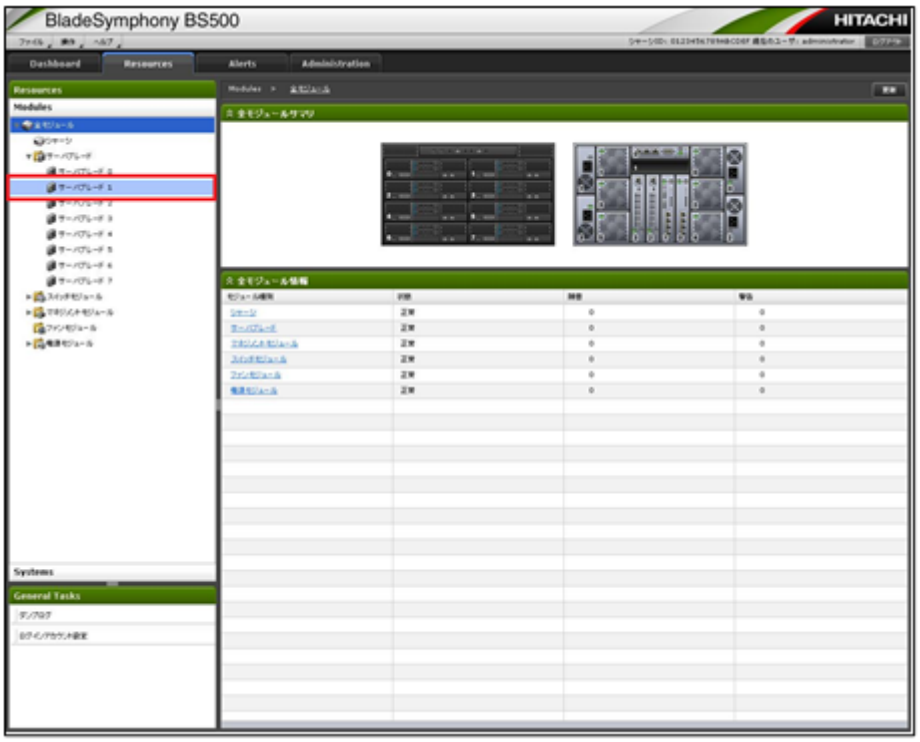
2.19.11 リモートコンソールの呼び出し

リモートコンソールを呼び出す手順を説明します。

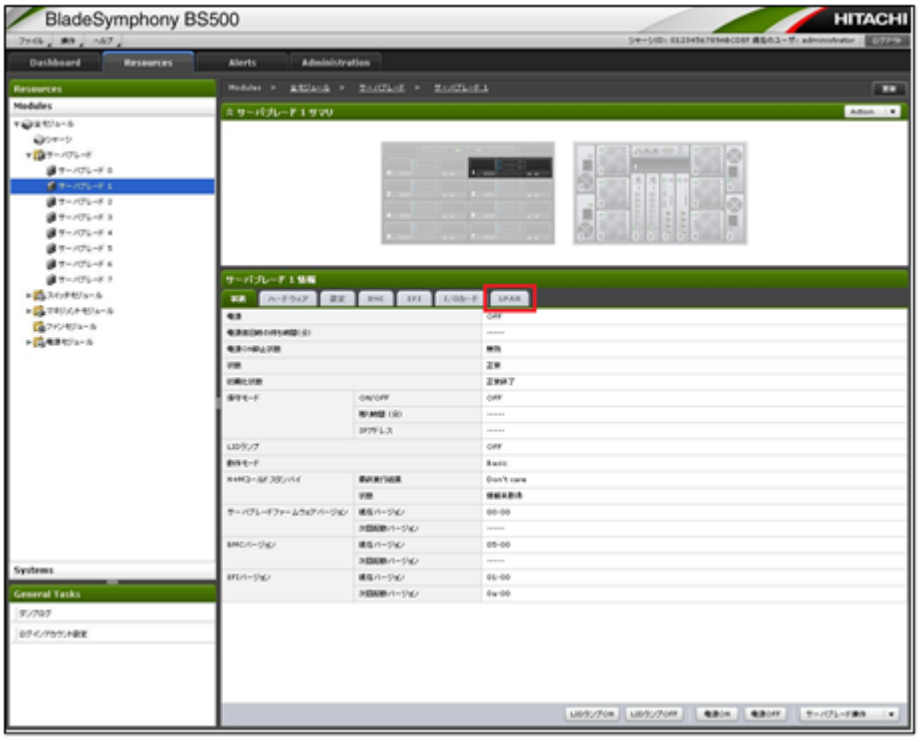
1. [Resources]タブをクリックします。



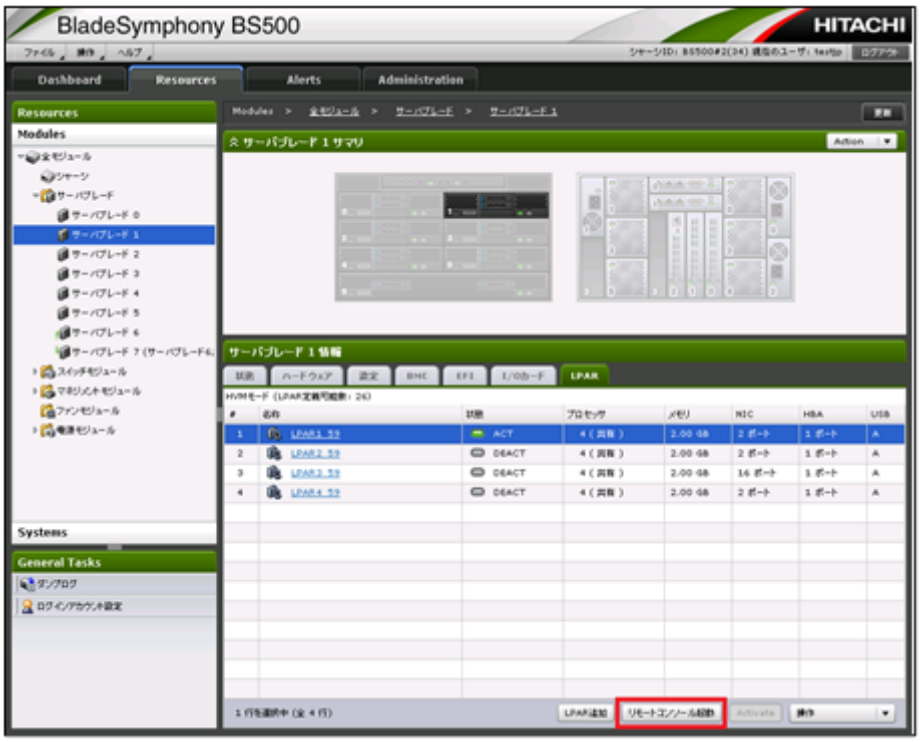
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブでリモートコンソールを割り当てる LPAR を選択し，[リモートコンソール起動]をクリックします。



参考 マネジメントモジュールファームウェアバージョンが A0125 より前のバージョンの場合，[R-KVM 起動]と表示されます。

5. [OK]ボタンをクリックします。

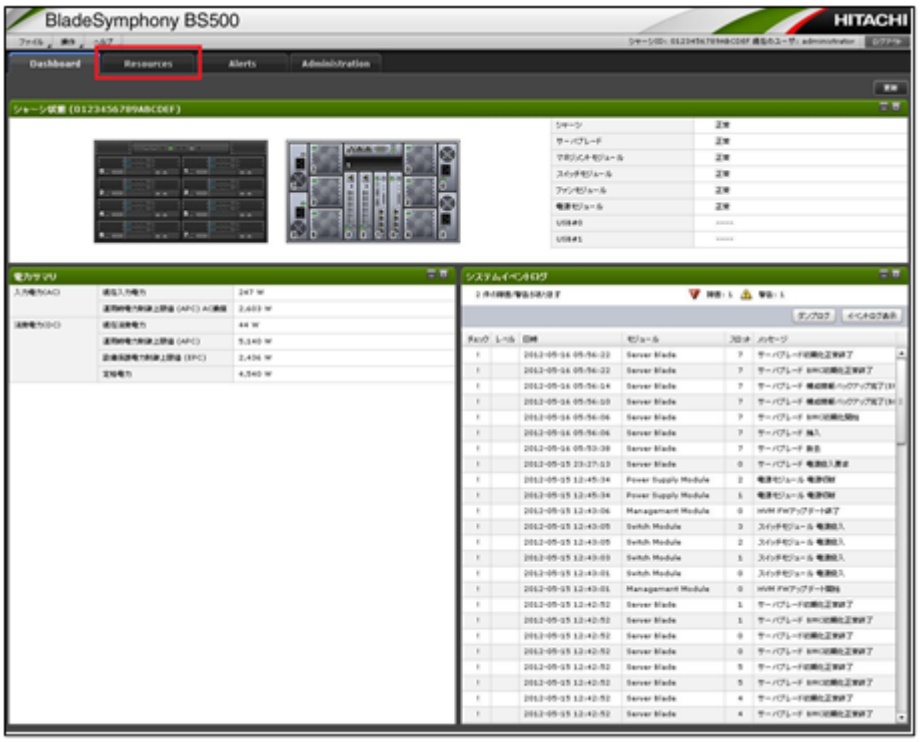
以上の操作により，リモートコンソールが表示されます。

2.19.12 LPAR の Reactivate

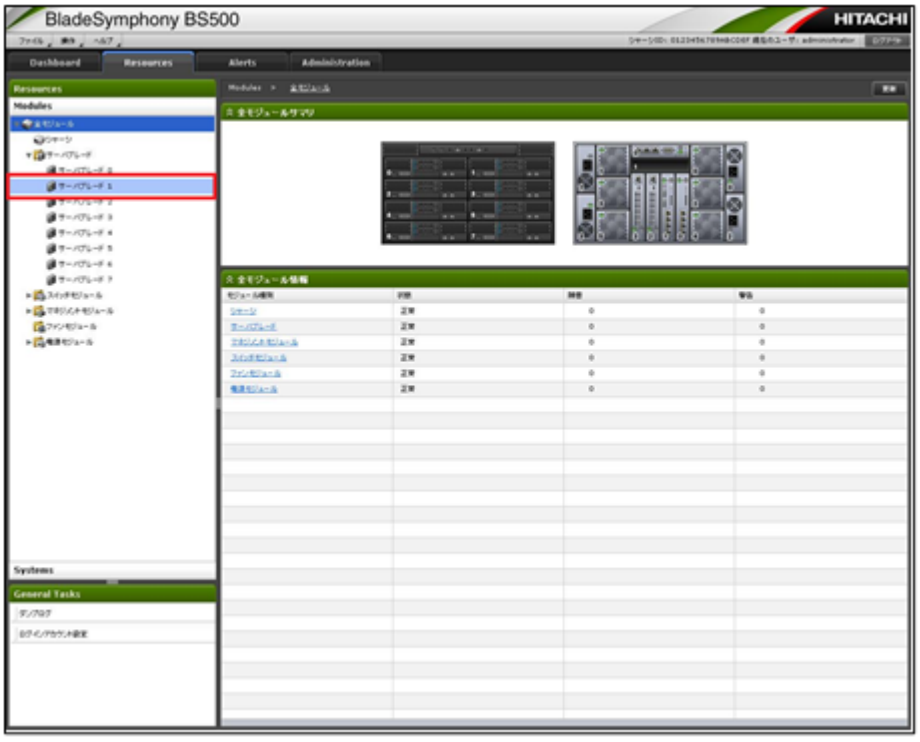
LPAR を Reactivate すると，LPAR 上で稼働しているゲスト OS は，強制的に再起動されます。LPAR の Reactivate を実施する前に，必ずゲスト OS の状態を確認してください。ゲスト OS を正常に再起動するには，ゲスト OS 上で再起動操作をしてください。

LPAR を Reactivate する手順を説明します。

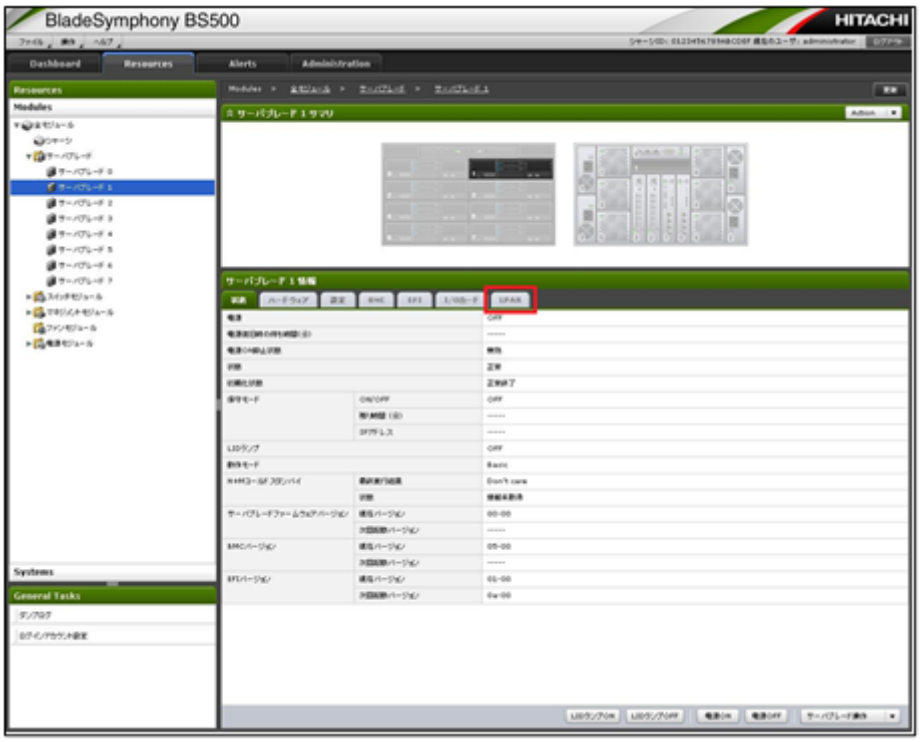
1. [Resources]タブをクリックします。



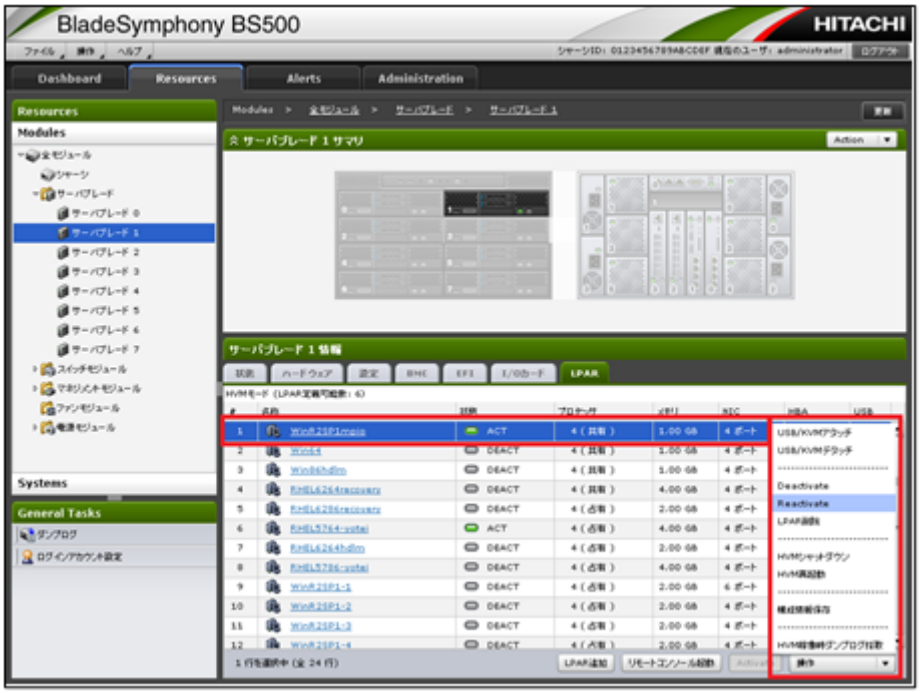
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブで Reactivate する LPAR を選択し，[操作]コンボボックスで[Reactivate]をクリックします。



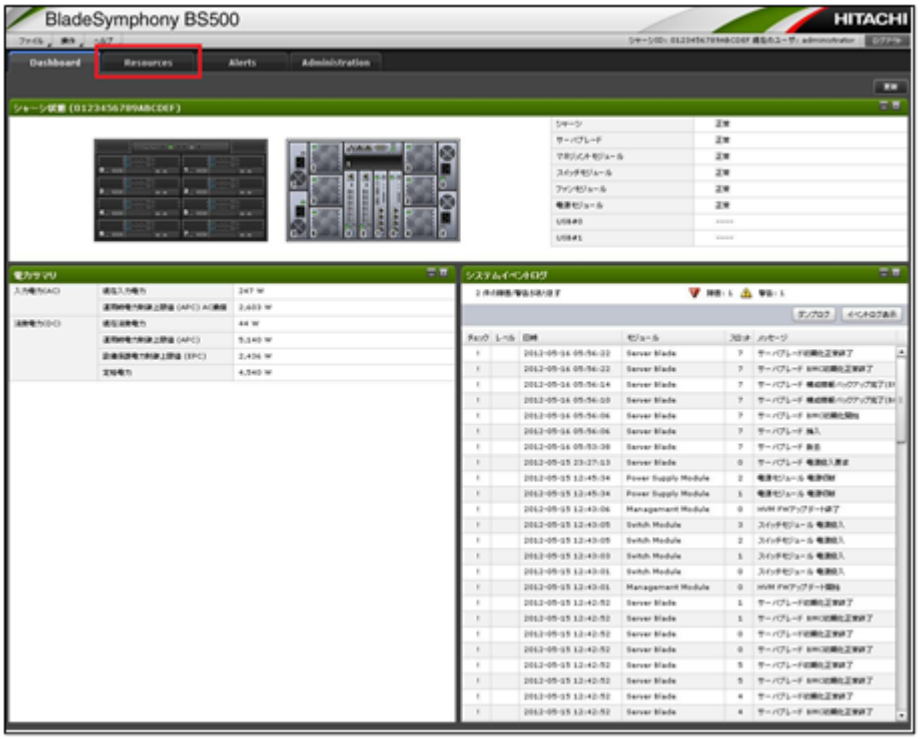
5. [OK]ボタンをクリックします。

2.19.13 LPAR の Deactivate

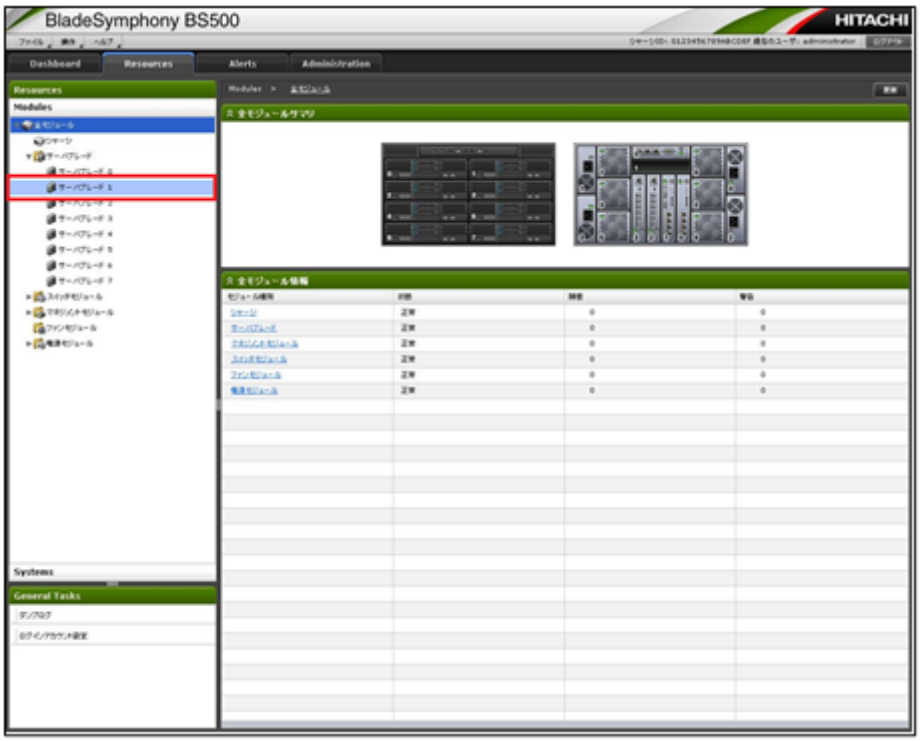
LPAR を Deactivate すると，LPAR 上で稼働しているゲスト OS を強制的にシャットダウンします。LPAR の Deactivate を実施する前に，必ずゲスト OS の状態を確認してください。ゲスト OS を正常にシャットダウンするには，ゲスト OS 上でシャットダウン操作をしてください。

LPAR を Deactivate する手順を説明します。

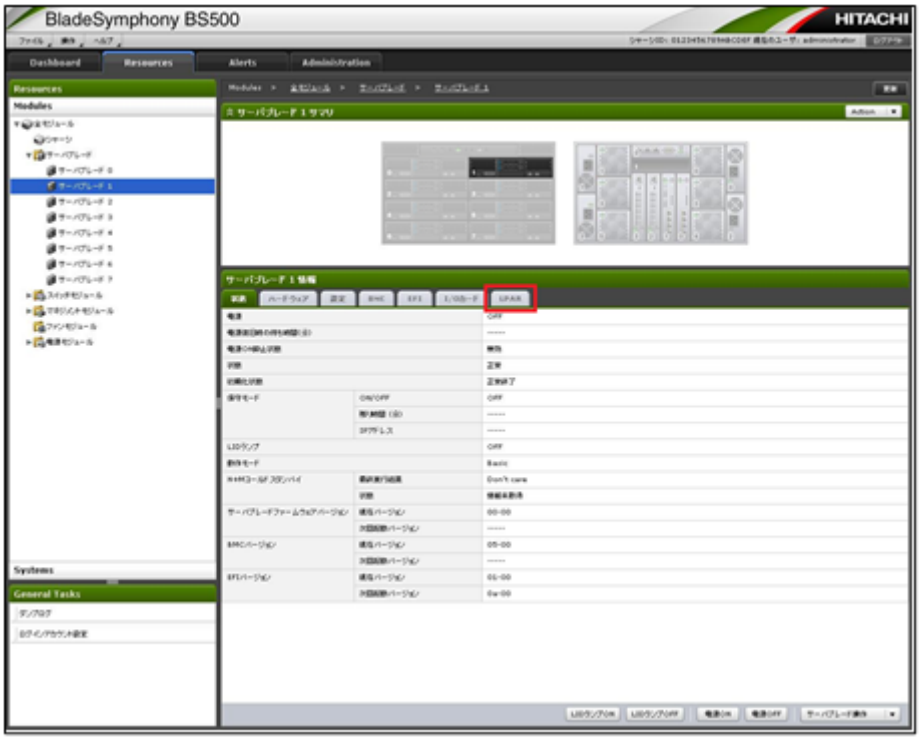
1. [Resources]タブをクリックします。



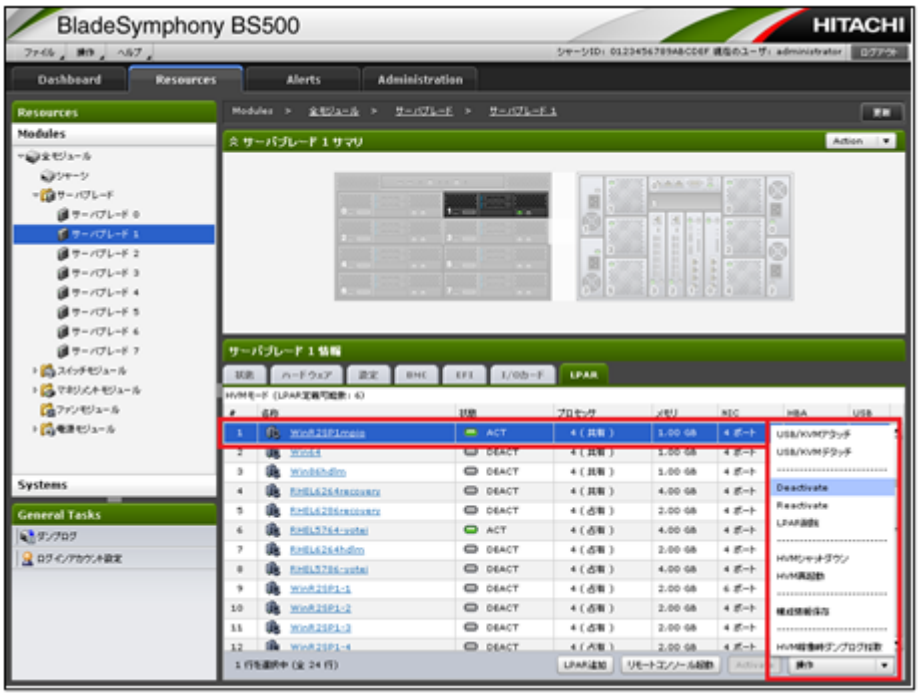
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブで Deactivate する LPAR を選択し，[操作]コンボボックスで[Deactivate]をクリックします。



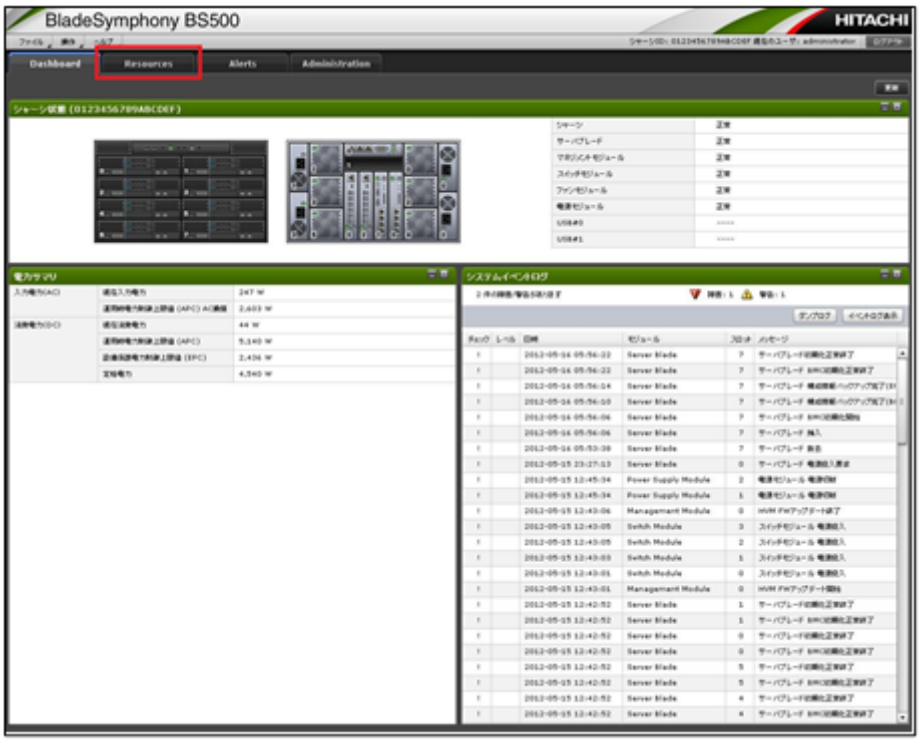
5. [OK]ボタンをクリックします。

2.19.14 LPAR 設定の変更

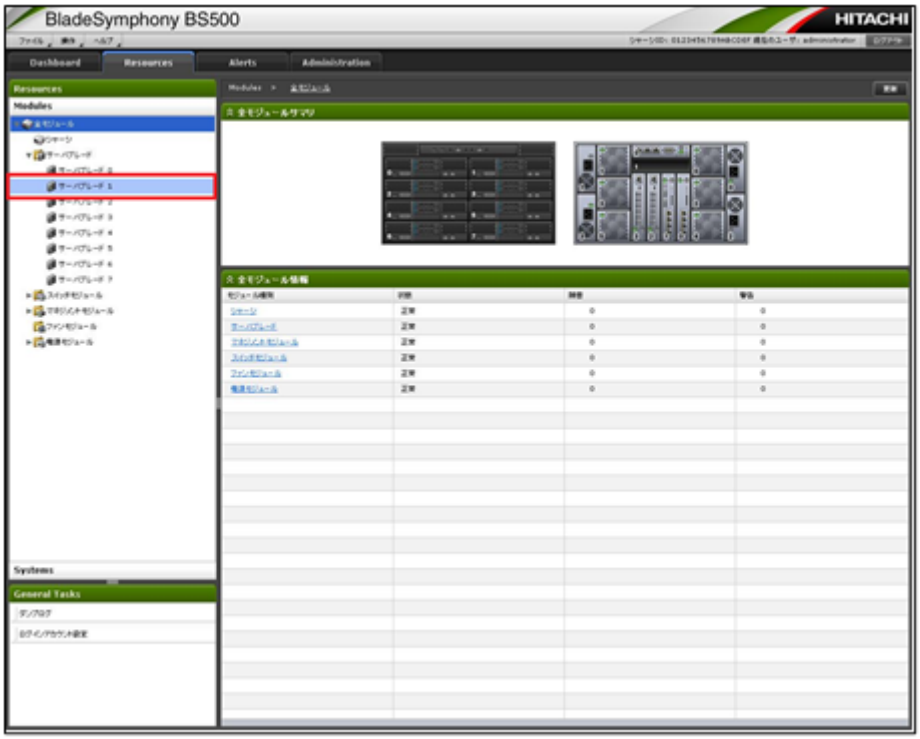
LPAR の設定を変更する手順を説明します。

なお，LPAR の状態が DEACT の場合に，LPAR の設定を変更することができます。

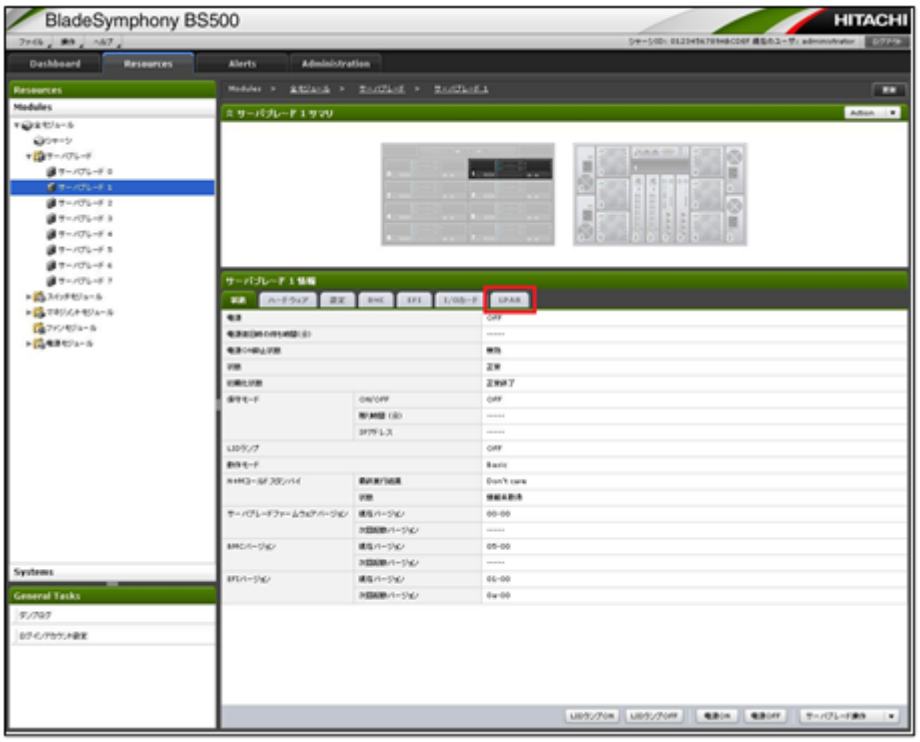
1. [Resources]タブをクリックします。



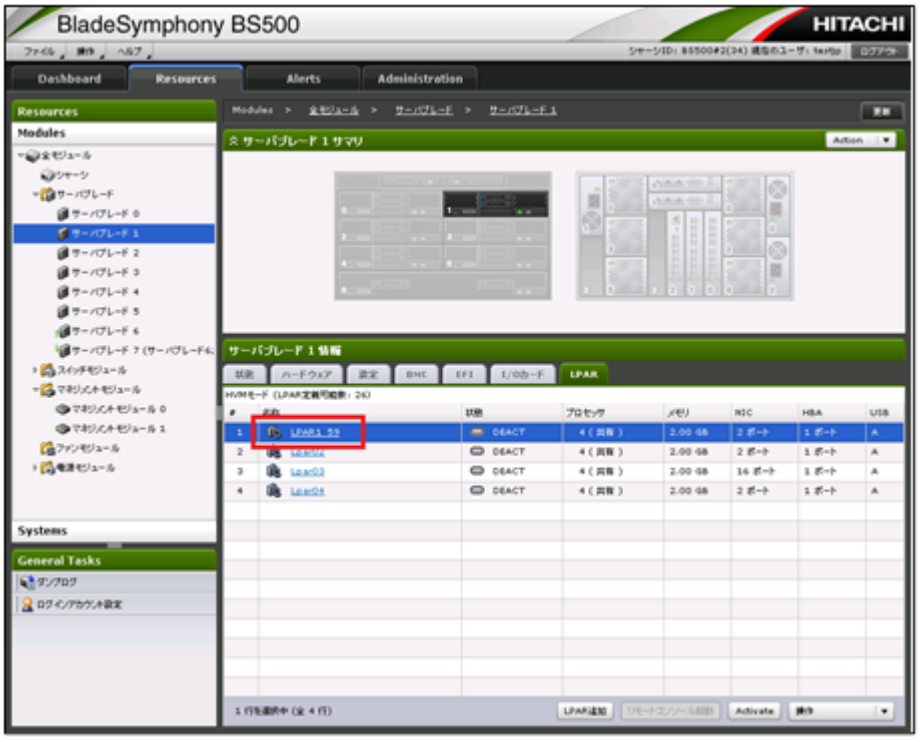
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



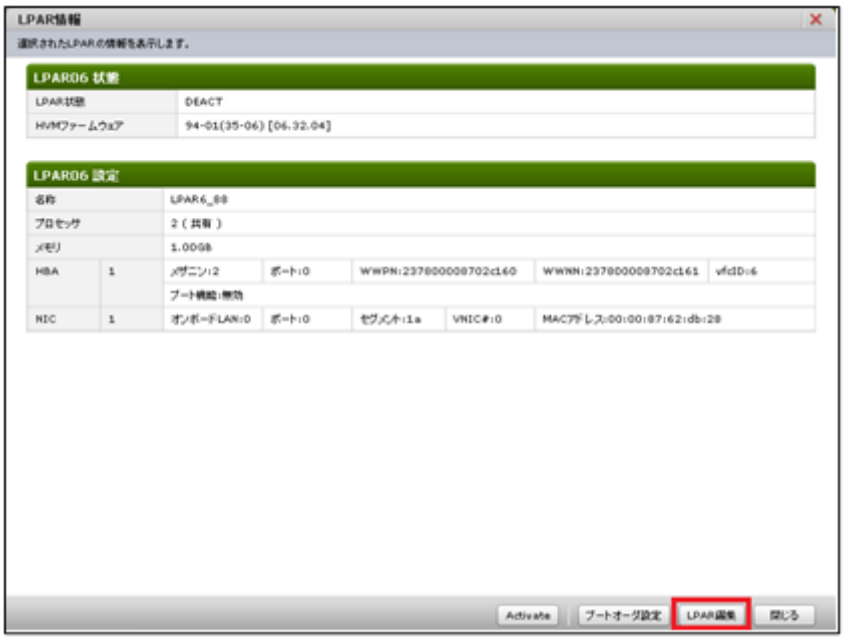
3. [サーバブレード]パネルの[LPAR]タブを選択します。



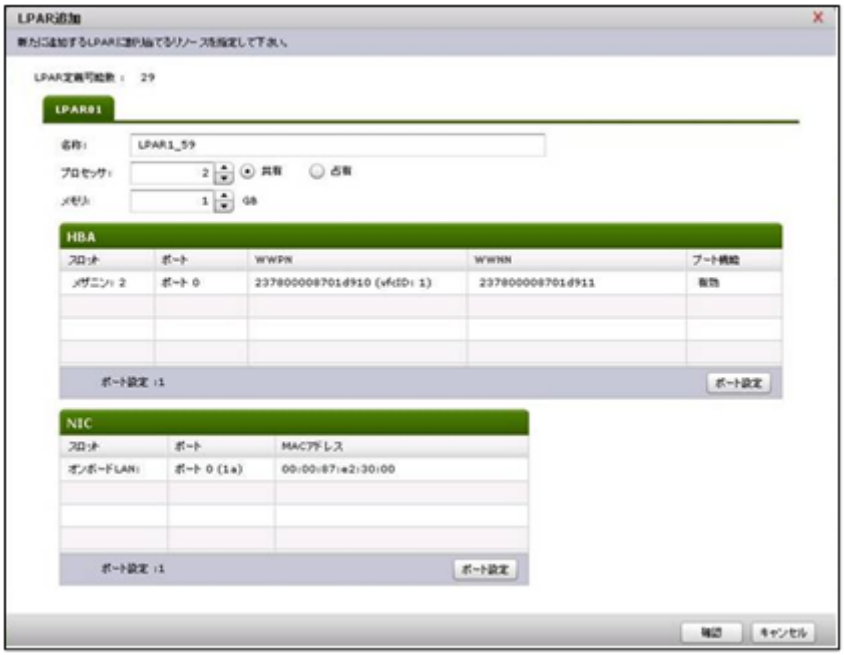
4. [LPAR]タブで設定変更対象 LPAR の LPAR 名をクリックします。



5. 設定内容を確認し，[LPAR 編集]をクリックします。



6. [LPAR 編集]画面が表示されます。
   以降の操作については「2.19.6 LPAR 作成」を参照してください。



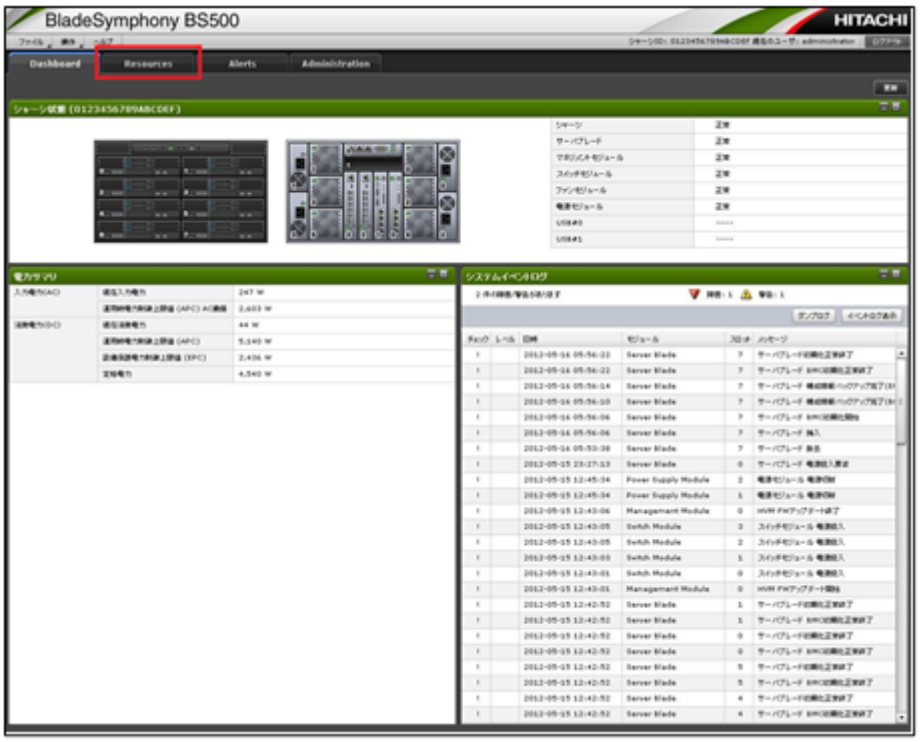
参考 LPAR 設定完了後は，HVM 構成情報を保存してください。HVM 構成情報の保存方法については，「2.19.7 HVM 構成情報の保存」を参照してください。

2.19.15 LPAR の削除

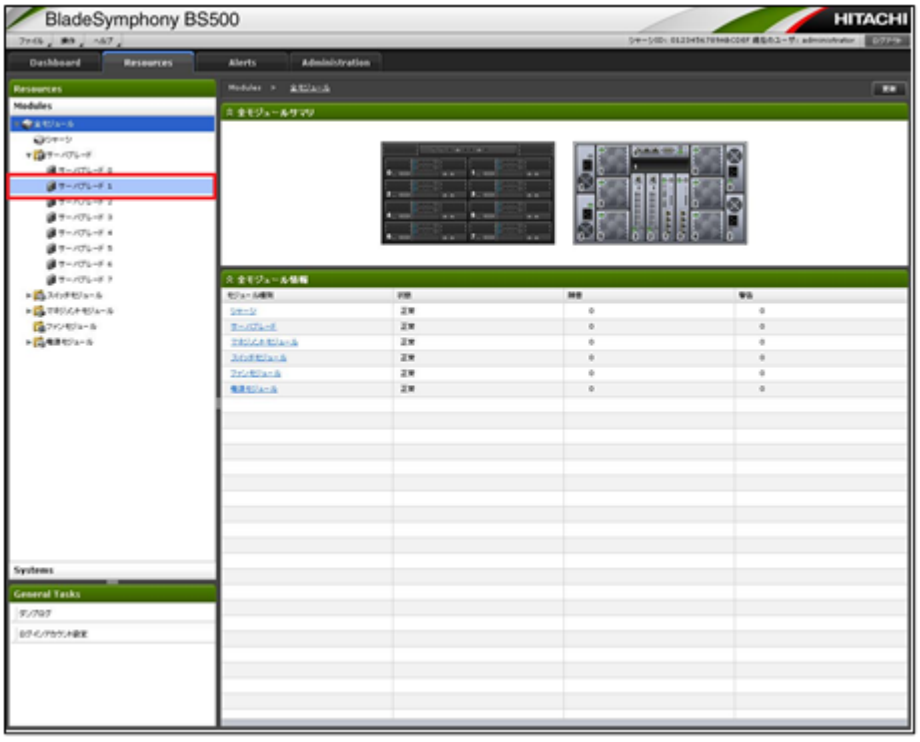
LPAR を削除する手順を説明します。

なお，LPAR の状態が DEACT の場合に，LPAR を削除することができます。

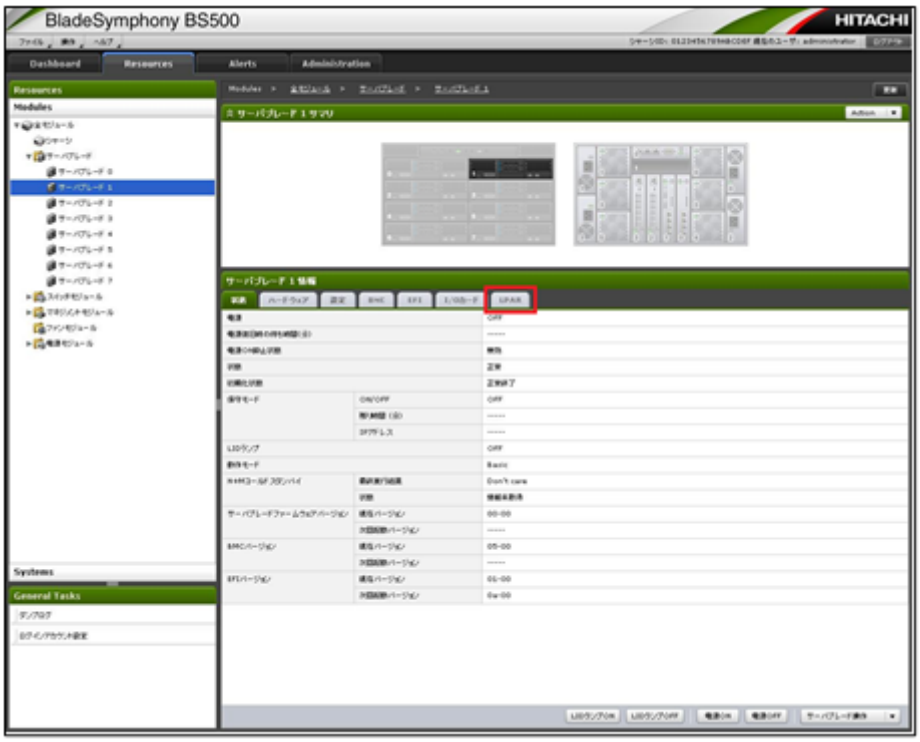
1. [Resources]タブをクリックします。



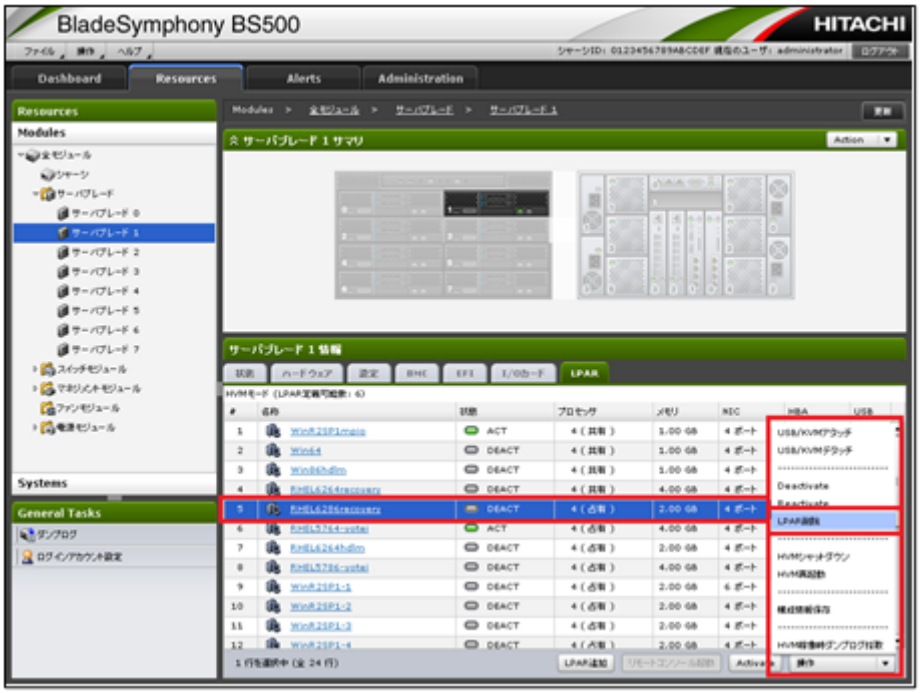
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブで削除する LPAR を選択し，[操作]コンボボックスで[LPAR 削除]をクリックします。



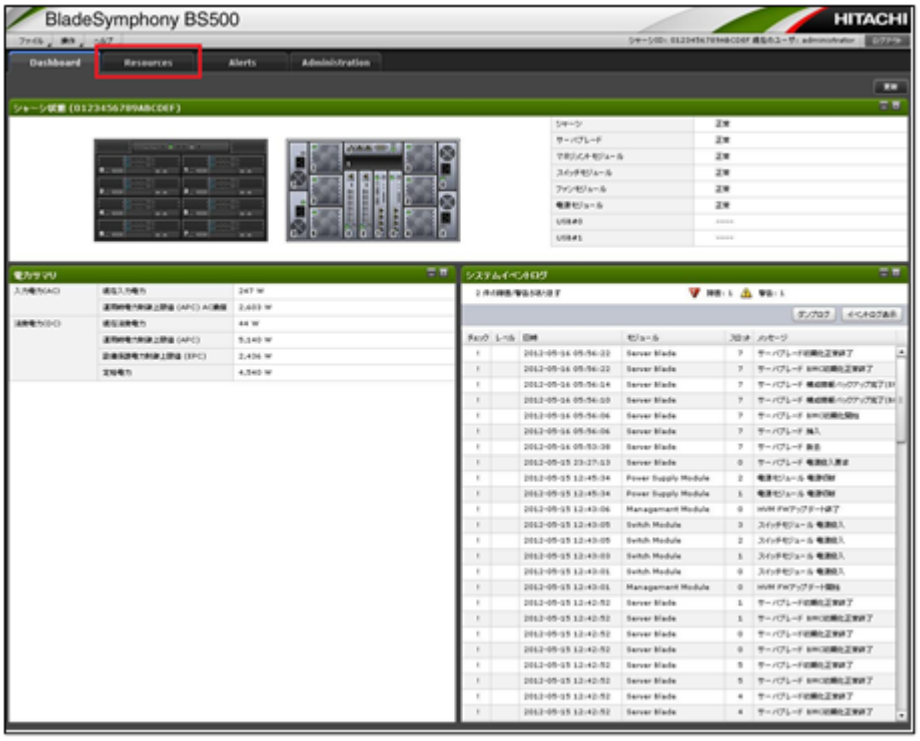
5. [OK]ボタンをクリックします。

2.19.16 HVM の再起動

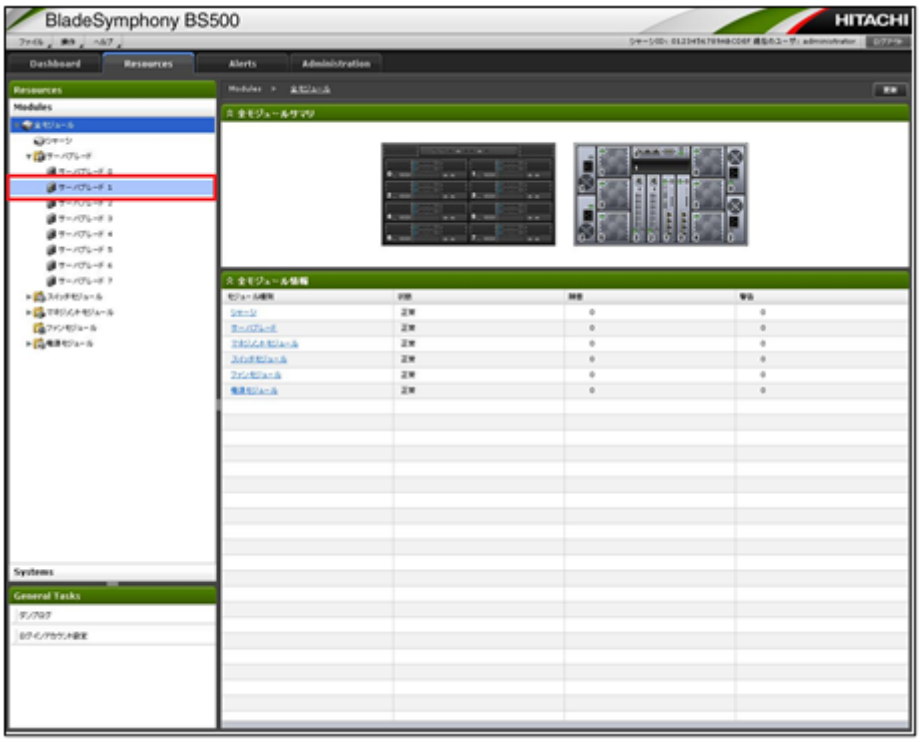
HVM を再起動する手順を説明します。

なお，すべての LPAR の状態が DEACT の場合に，HVM を再起動することができます。

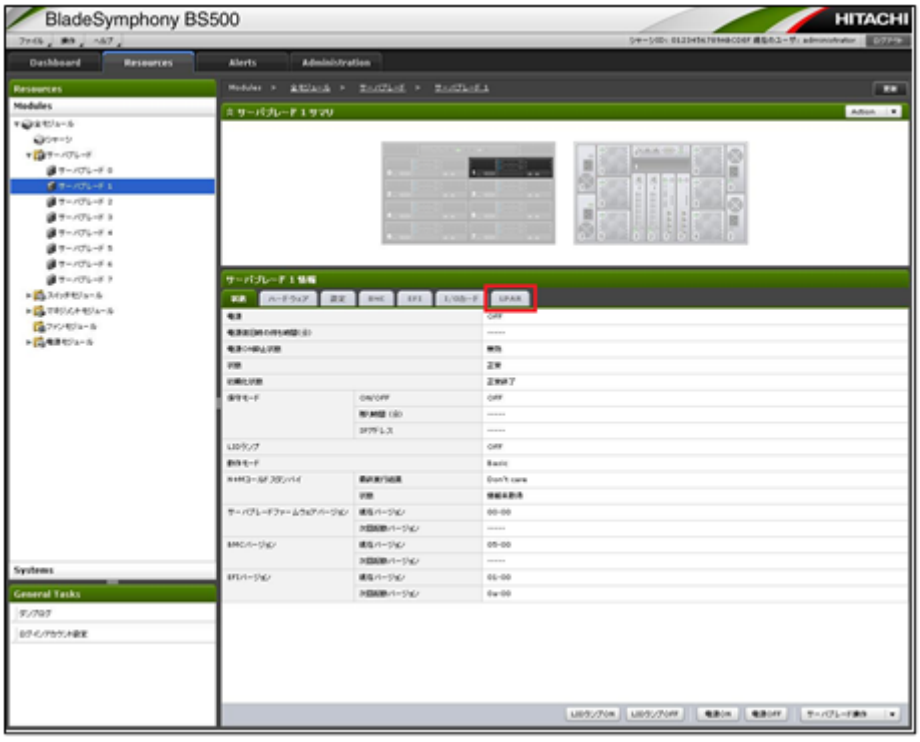
1. [Resources]タブをクリックします。



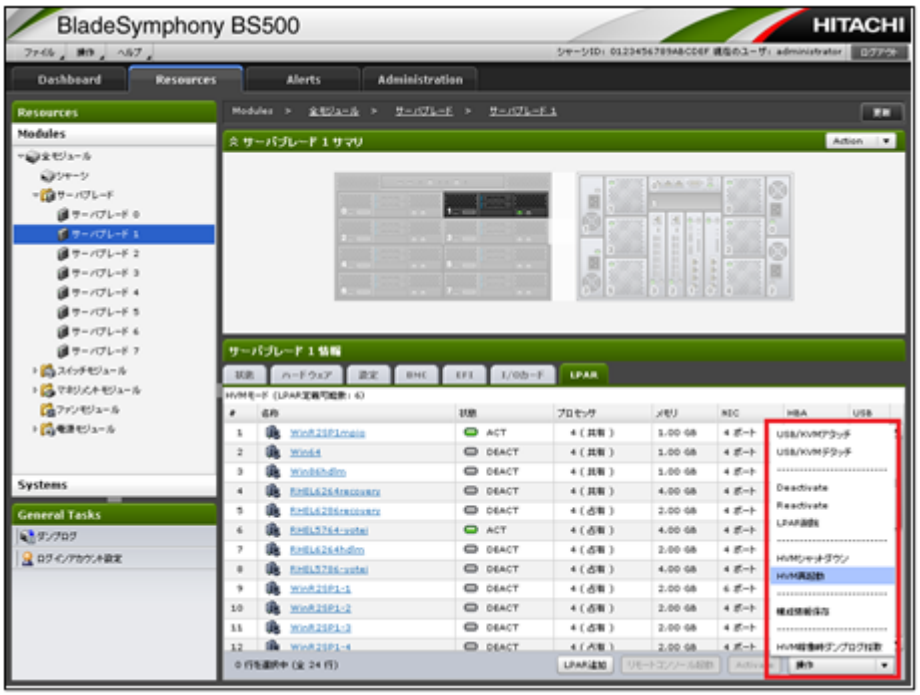
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブにある[操作]コンボボックスで[HVM 再起動]をクリックします。



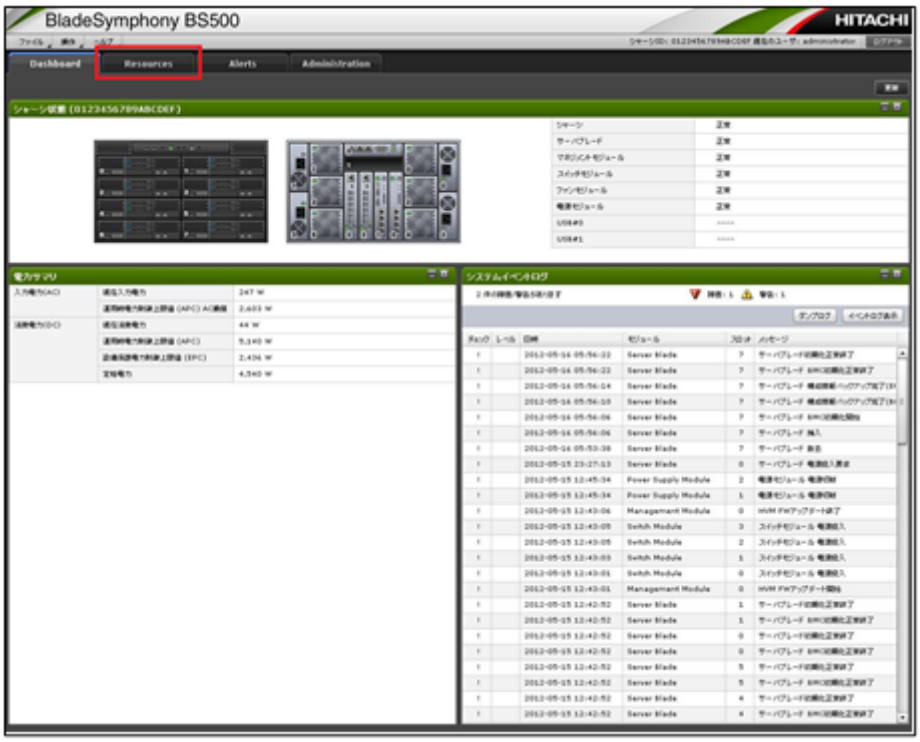
5. [OK]ボタンをクリックします。

2.19.17 HVM のシャットダウン

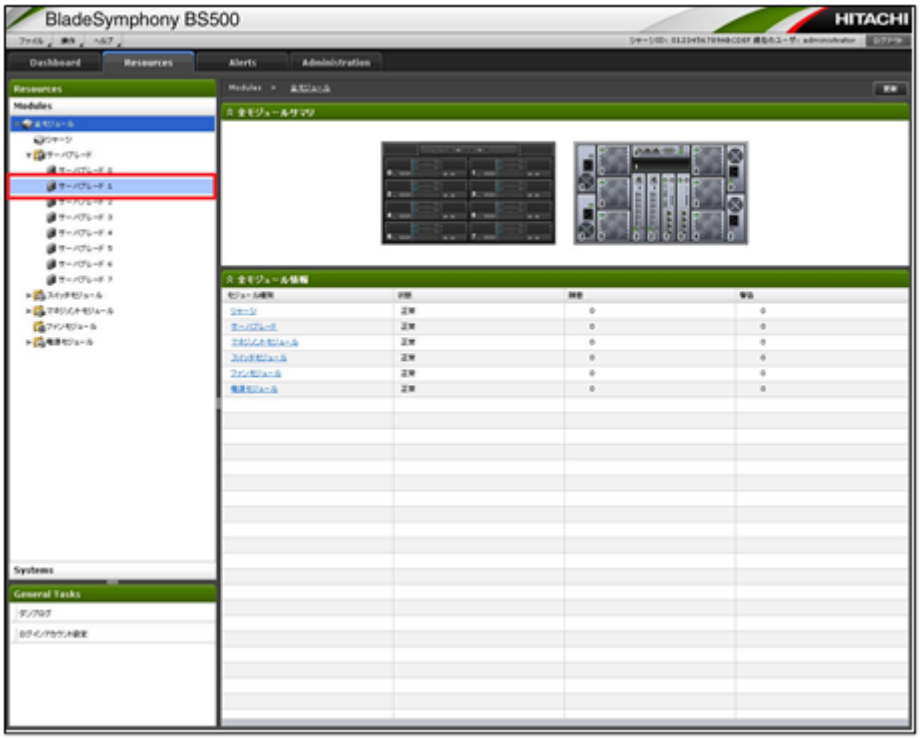
HVM をシャットダウンする手順を説明します。

なお，すべての LPAR の状態が DEACT の場合に，HVM をシャットダウンすることができます。

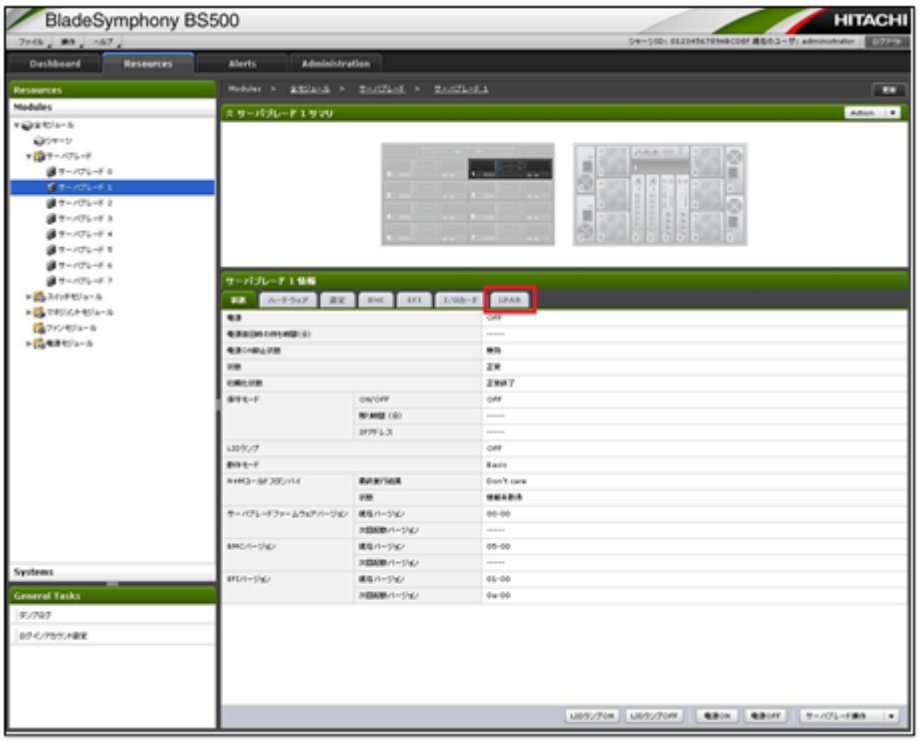
1. [Resources]タブをクリックします。



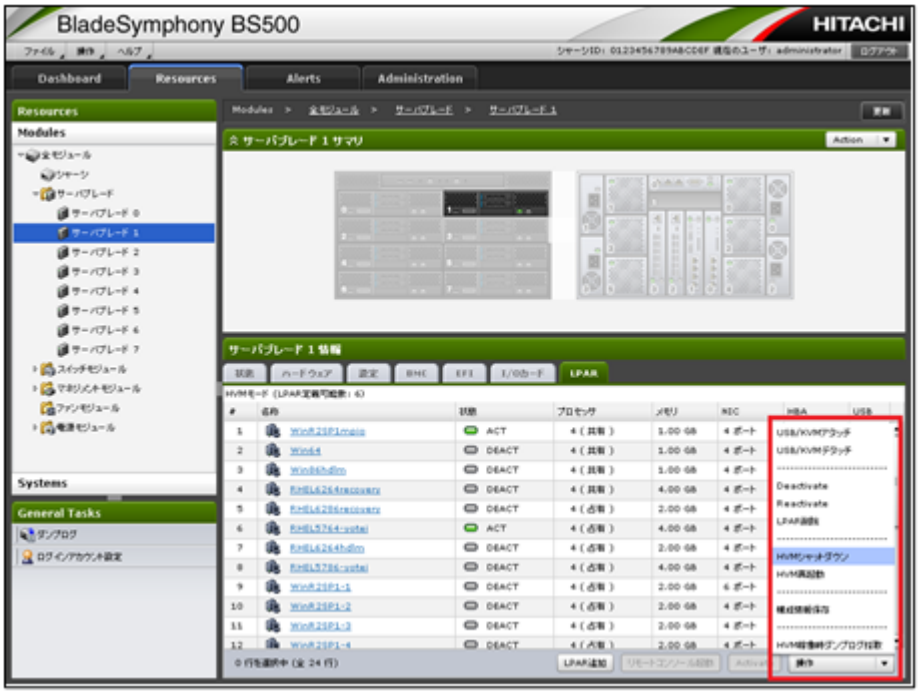
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブにある[操作]コンボボックスで[HVM シャットダウン]をクリックします。



5. [OK]ボタンをクリックします。

6. HVM をシャットダウンする前に HVM 構成情報を保存するため，[保存]ボタンをクリックします。

7. [OK]ボタンをクリックします。

8. [閉じる]ボタンをクリックします。

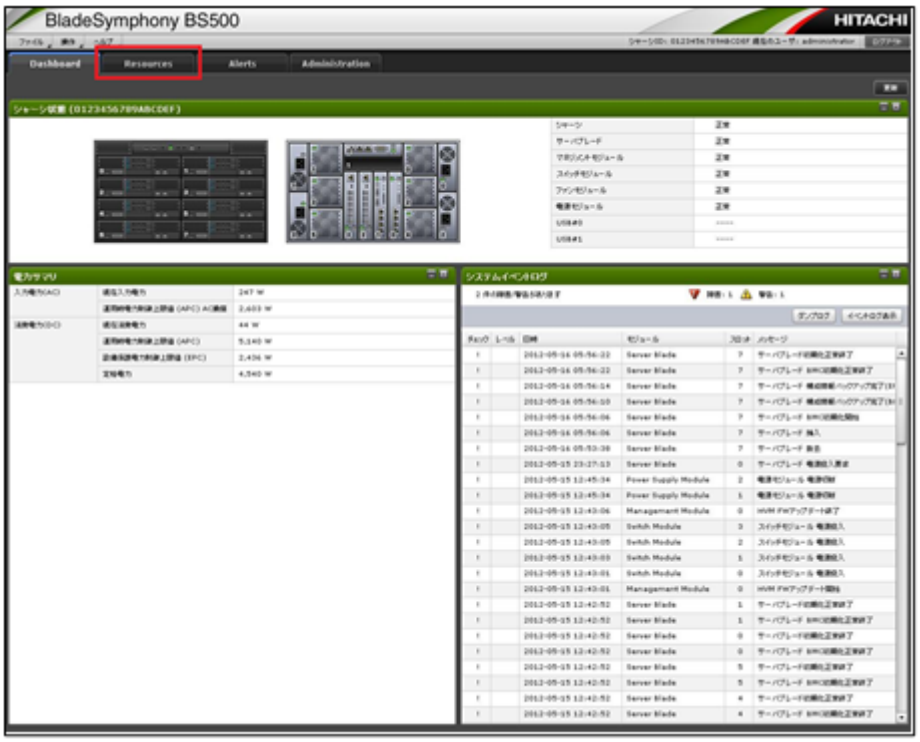
9. [HVM シャットダウン]ボタンをクリックします。

10. [閉じる]ボタンをクリックします。

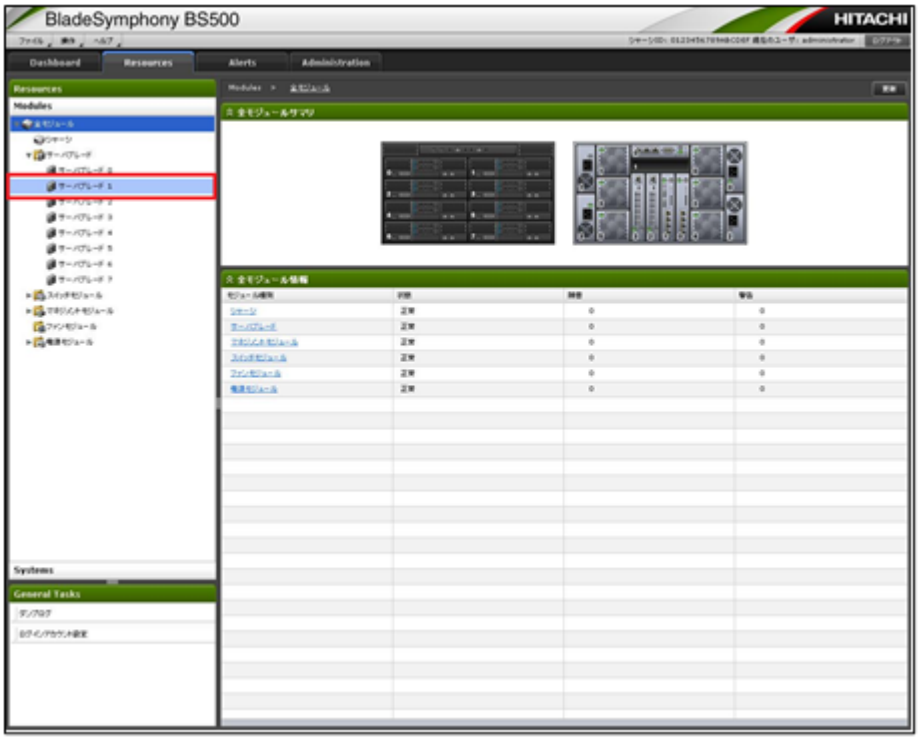
2.19.18 HVM 設定のバックアップ

HVM 設定をバックアップする手順を説明します。

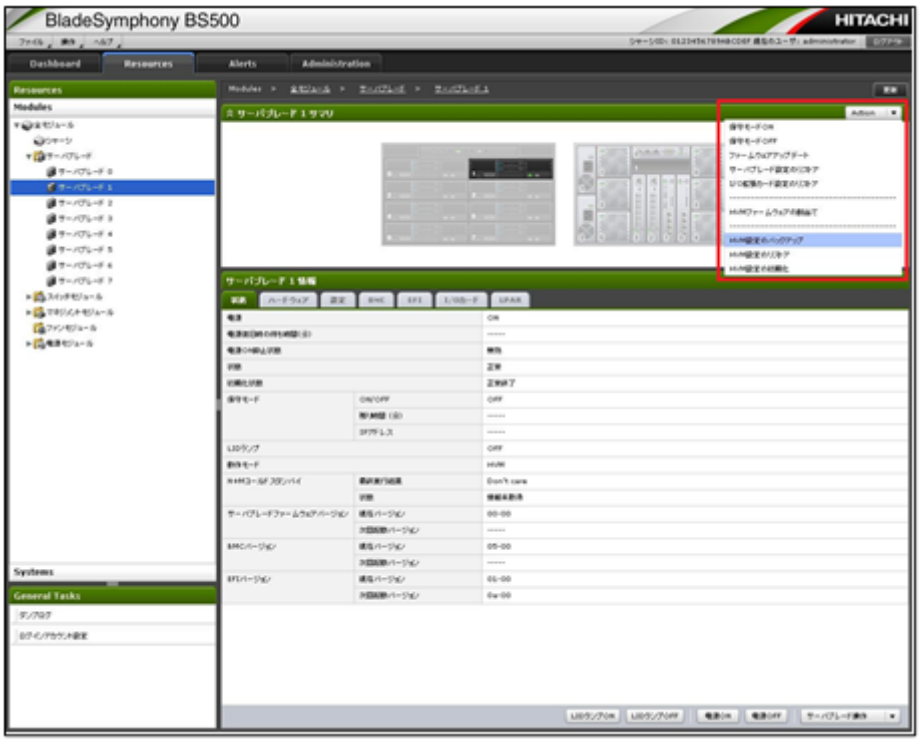
1. [Resources]タブをクリックします。



2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレードサマリ]パネルの[Action]コンボボックスで[HVM 設定のバックアップ]をクリックします。



4. [保存]ボタンをクリックします。

参考

- ファイルの保存手順については，OS の操作手順に従ってください。
- 【マネジメントモジュールファームウェアバージョン A0145 以降】
  ファイル名称は次のようになります。
  hvm-pX-VVRR-YYYYMMDDhhmmss.backup
  ここで，X はパーティション(サーバブレード)番号，VVRR は現在割り当てられている HVM バージョンが入ります。
- SMP 構成の場合は，プライマリサーバブレードを選択してください。

2.19.19 HVM 設定のリストア

HVM 設定のリストアを行う場合，次の要件を満たしたバックアップファイルを適用してください。

（1）同一 HVM のバックアップファイルであること

（2）現在の HVM ファームウェアバージョンが割り当てられていた時にバックアップしたファイルであること

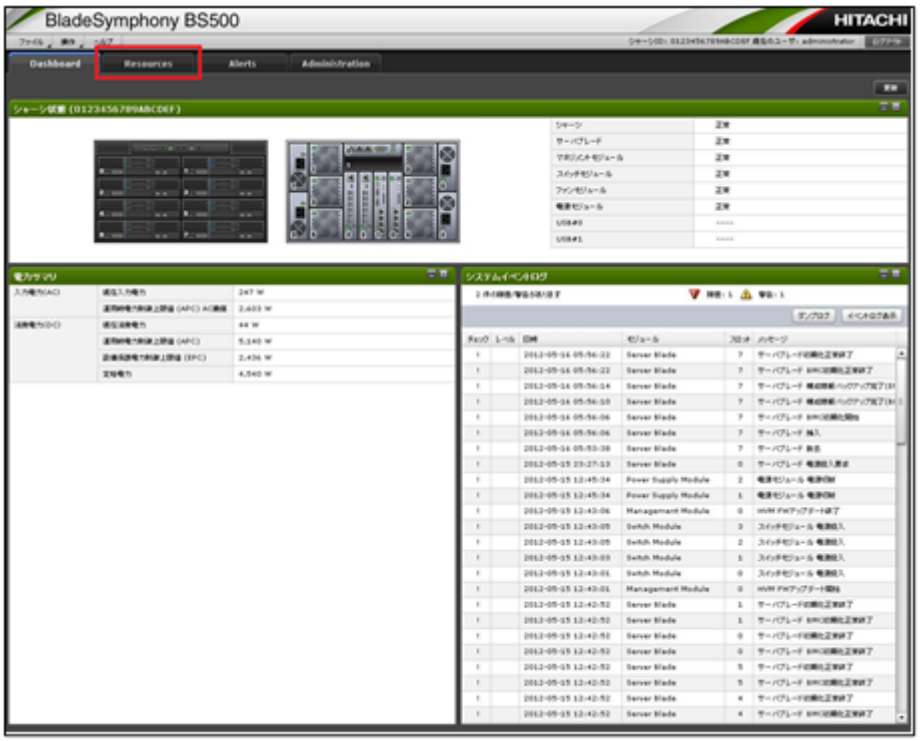
これらの要件を満たしていないファイルを用いた場合，HVM が正常に動作しないことがあります。

HVM 設定をリストアする手順を説明します。

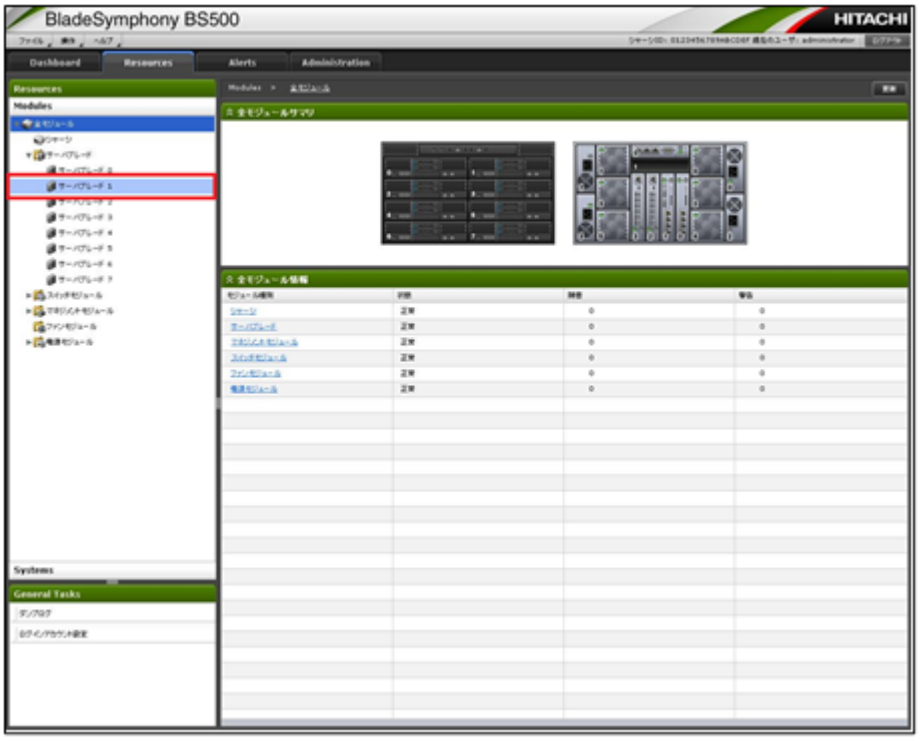
参考 SMP 構成の場合は，プライマリサーバブレードを選択してください。

なお，サーバブレードが電源 OFF の場合に，HVM 設定をリストアすることができます。

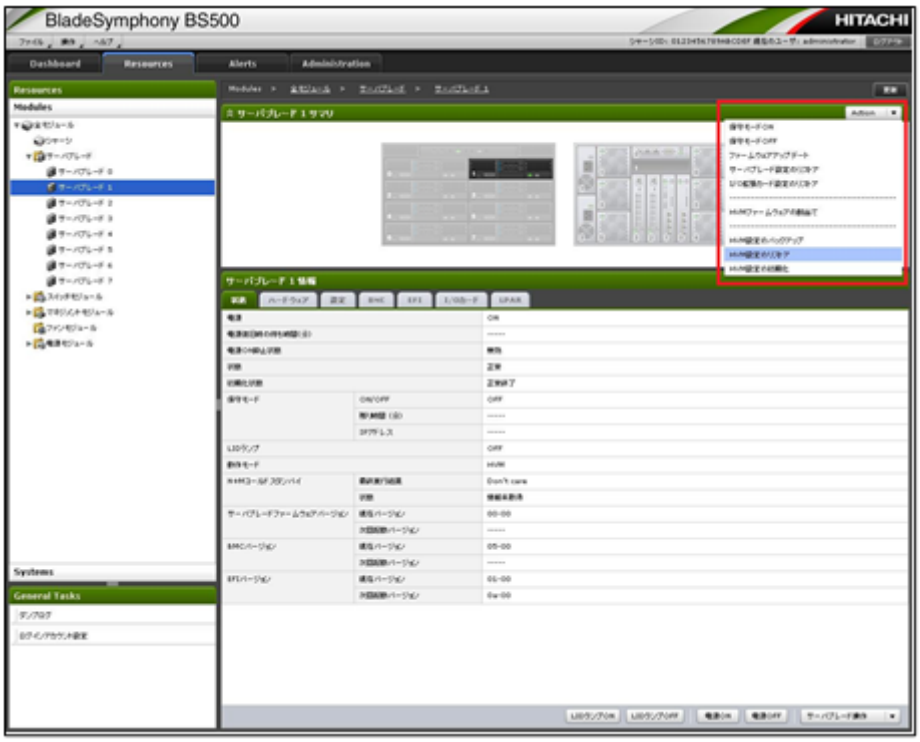
1. [Resources]タブをクリックします。



2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレードサマリ]パネルの[Action]コンボボックスで[HVM 設定のリストア]をクリックします。



4. [参照]ボタンをクリックします。

参考 ファイルを開く手順については，OS の操作手順に従ってください。

5. [確認]ボタンをクリックします。

6. [OK]ボタンをクリックします。

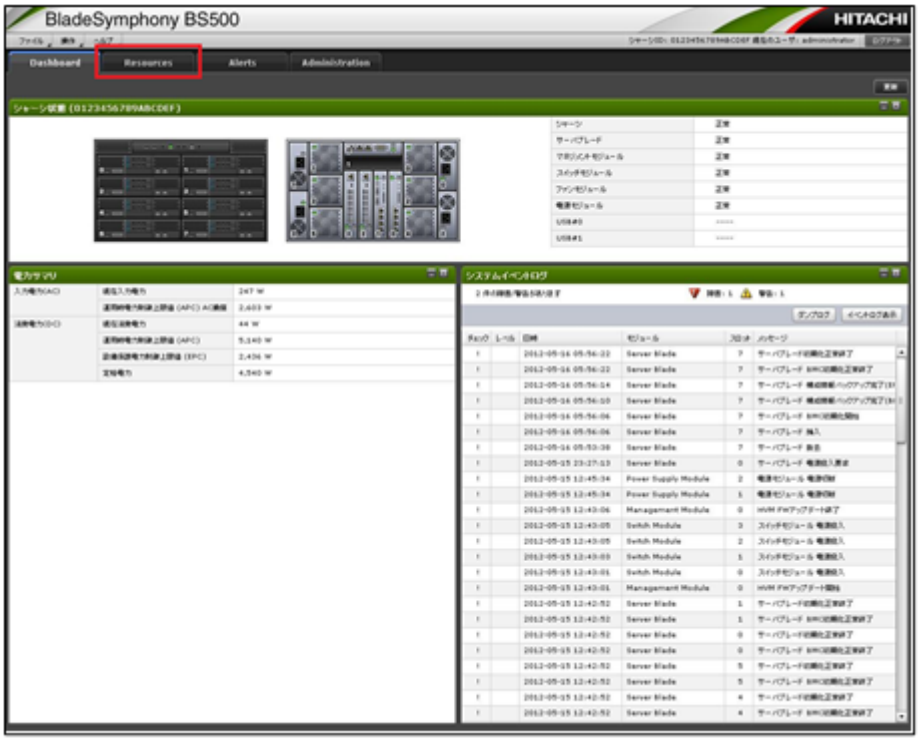
7. [閉じる]ボタンをクリックします。

2.19.20 HVM 設定の初期化

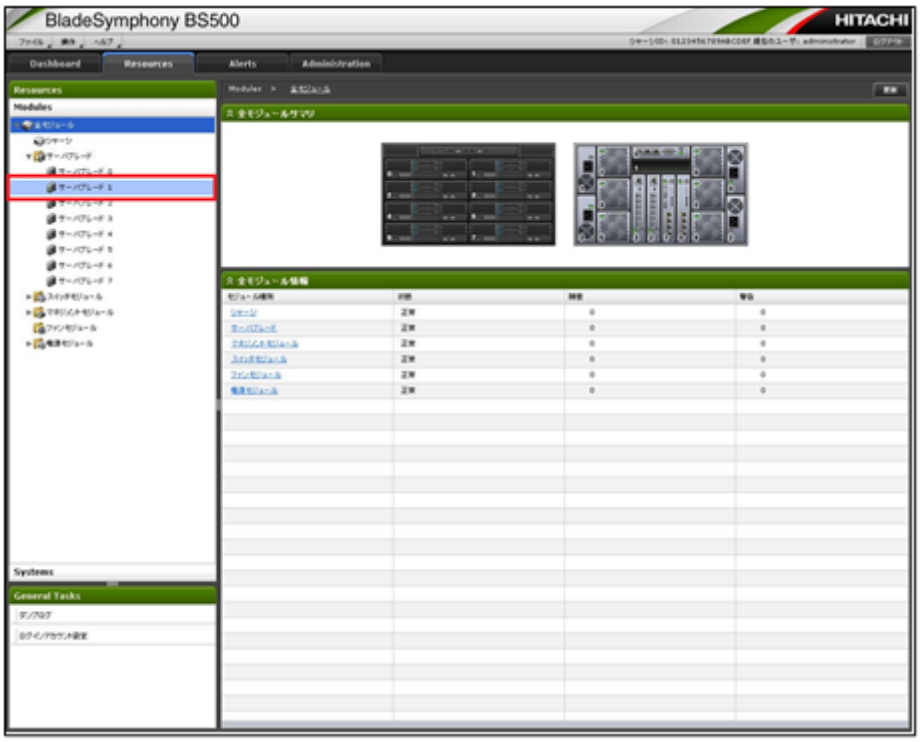
HVM 設定を初期化する手順を説明します。なお，サーバブレードが電源 OFF の場合に，HVM 設定を初期化することができます。

HVM 設定を初期化すると，HVM 構成情報はすべて消えてしまいます。HVM 設定の初期化前には，HVM 構成情報をバックアップすることを推奨します。

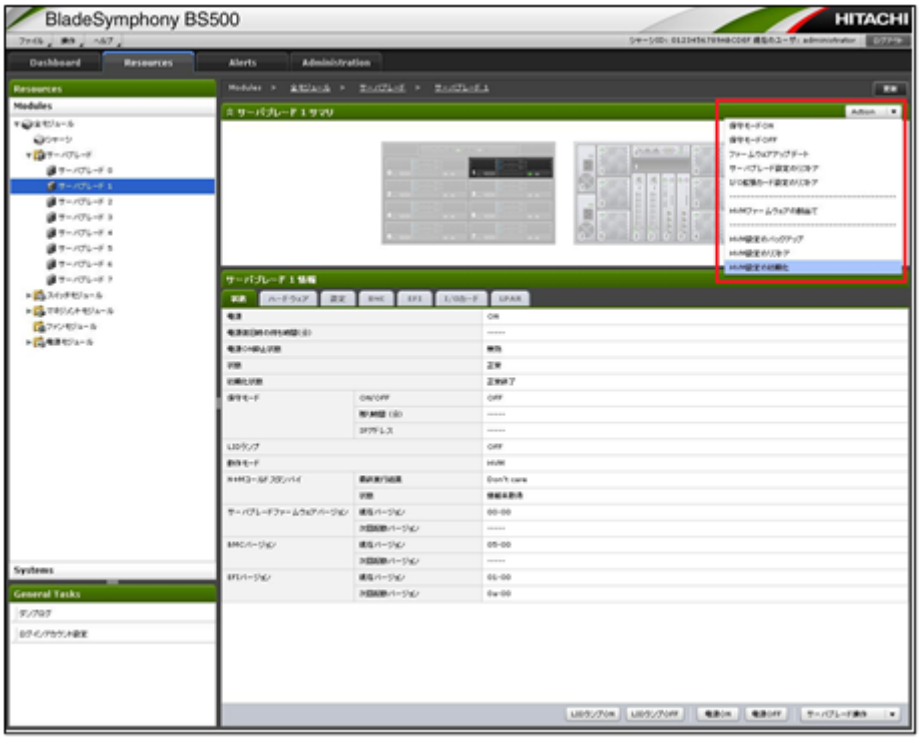
1. [Resources]タブをクリックします。



2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレードサマリ]パネルの[Action]コンボボックスで[HVM 設定の初期化]をクリックします。



4. [OK]ボタンをクリックします。

5. [OK]ボタンをクリックします。

2.19.21 HVM のモデルアップ

HVM のモデルアップ手順を説明します。

参考

- HVM をモデルアップするためには, HVM ライセンスキーを取得し, Web コンソールでそのライセンスキーを HVM に適用する必要があります。

  HVM ファームウェアのモデルアップ手順は次のとおりです。なお，HVM ライセンスキーを登録する際は，サーバブレードの電源が OFF である必要があります。
- SMP 構成の場合，SMP を構成するすべてのサーバブレードの HVM をモデルアップする必要があります。

(1) HVM ライセンスキーの入手

HVM ライセンスキーの入手方法について説明します。

次のものを用意する必要があります。

- WAK（Web Access Key）

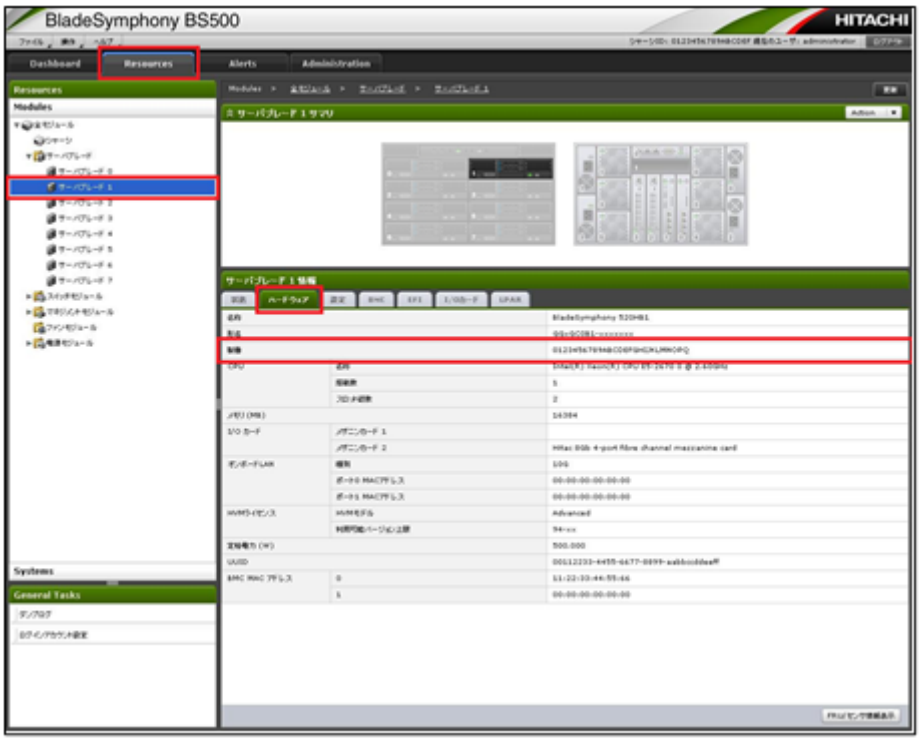
  弊社営業に問い合わせの上，Virtage Advanced ライセンス，または Virtage Enterprise ライセンスをご購入ください。
- ブレードシリアル番号

  Web コンソールで対象サーバブレードのブレードシリアル番号を確認してください。

参考

- ここでは，サーバブレードの製番をブレードシリアル番号と呼びます。
- サーバブレードの製番は次の手順で確認できます。

  [Resources]タブ－[Resources]パネル－[Modules]アコーディオン内のツリービューからサーバブレードを選択後，[サーバブレード情報]パネルで[ハードウェア]タブを選択すると，製番を表示します。



HVM ライセンスキーの入手方法

BladeSymphony ホームページより HVM ライセンスキー発行画面に移動し, HVM ライセンスキーを入手します。

ホームページアドレス:http://www.hitachi.co.jp/products/bladesymphony/

1. BladeSymphony ホームページより HVM ライセンスキー発行画面に移動します。次のように移動してください。

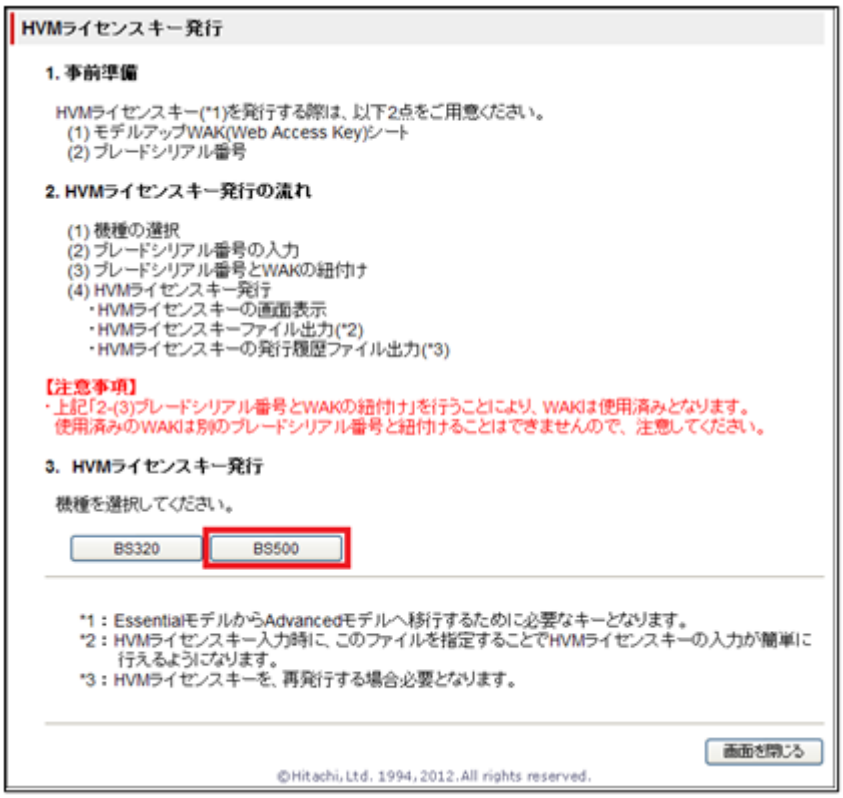
   [ダウンロード]

   ↓

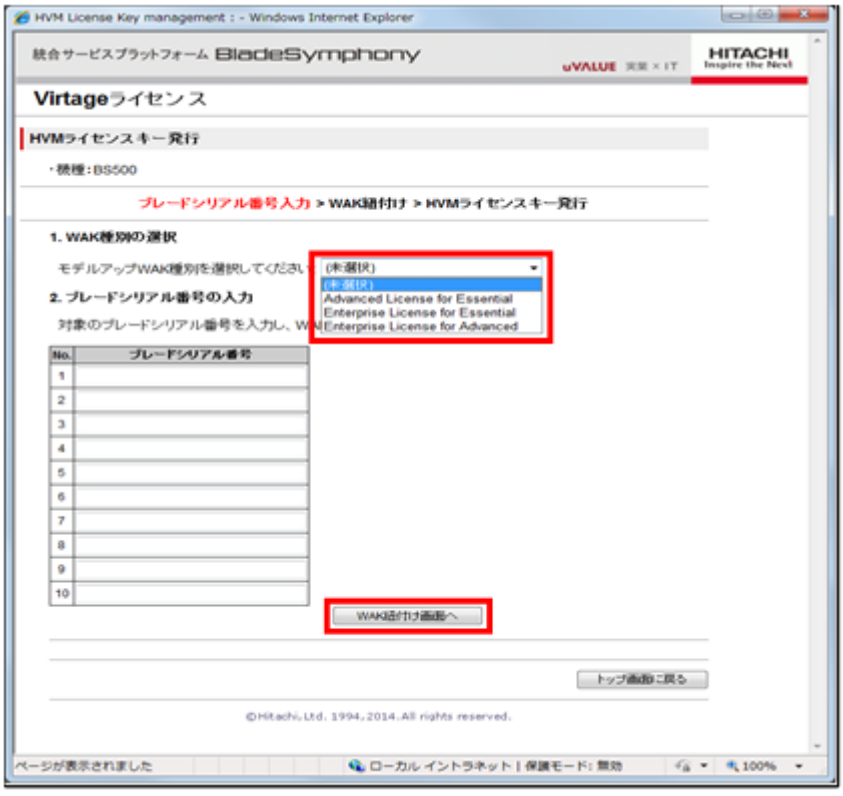
   [ライセンスキー]の[詳細はこちら]

   ↓

   [HVM ライセンスキー]
2. HVM ライセンスキー発行画面で[BS500]ボタンをクリックします。



3. モデルアップ WAK 種別を選択した後，ブレードシリアル番号を入力し，[WAK 紐付け画面へ] ボタンをクリックします。

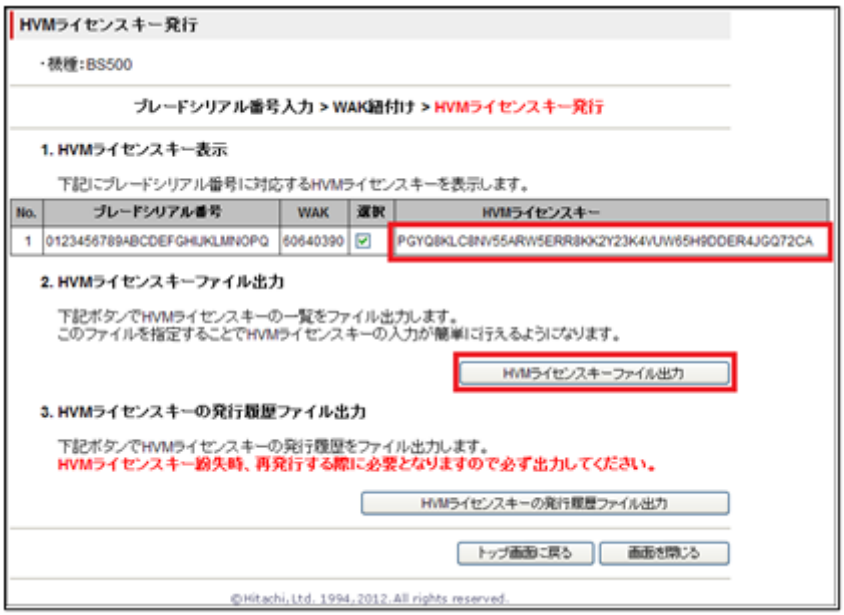


4. WAK を入力し，[HVM ライセンスキー発行画面へ]ボタンをクリックします。

5. HVM ライセンスキーを入手します。

「(2) HVM ライセンスキーの登録」で HVM ライセンスキーを直接入力する場合は，HVM ライセンスキーを控えておきます。

「(2) HVM ライセンスキーの登録」で HVM ライセンスキーファイルを読み込ませる場合は，[HVM ライセンスキーファイル出力]ボタンをクリックし，HVM ライセンスキーファイルをシステムコンソールのハードディスクに格納します。

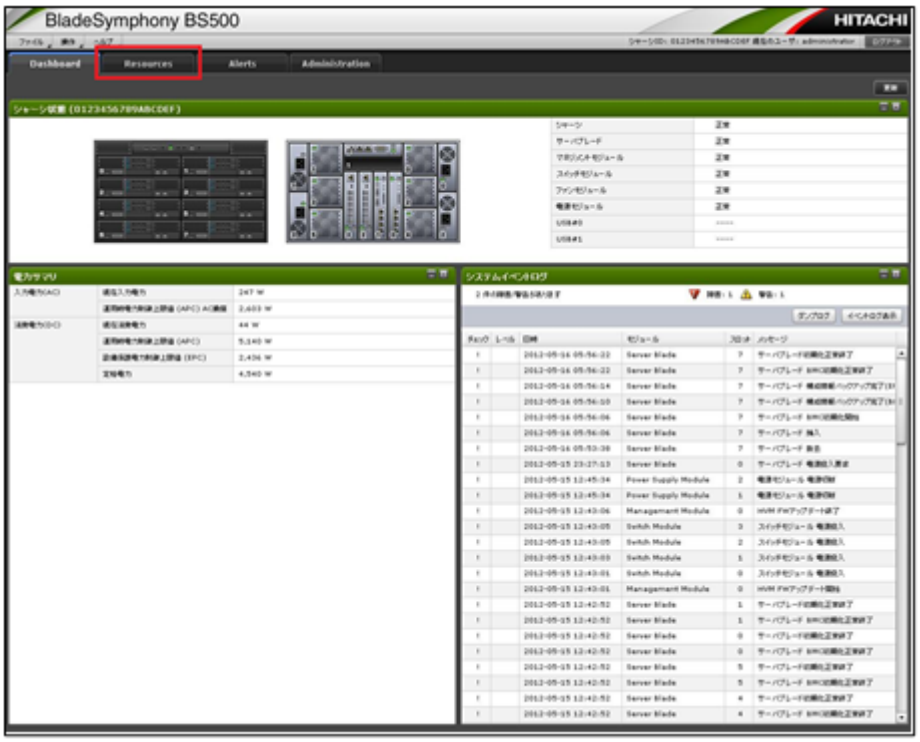


参考 HVM ライセンスキーファイルを再発行する際は，発行履歴ファイルに記録されたブレードシリアル番号と紐付け済み WAK を，発行時と同様の手順で入力してください。

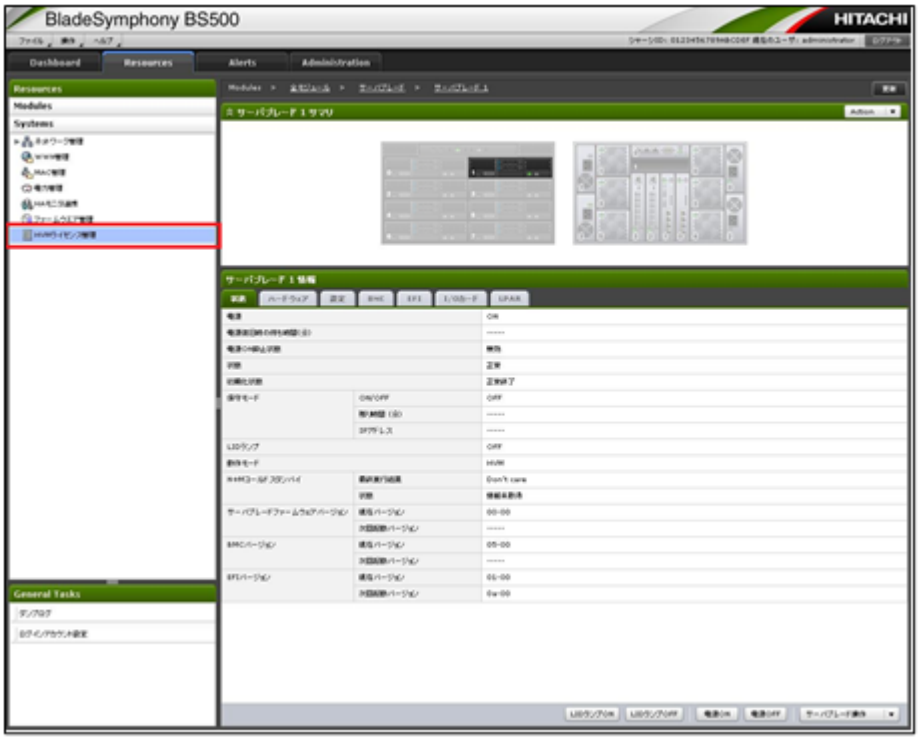
(2) HVM ライセンスキーの登録

サーバブレードの電源が OFF の場合に，HVM ライセンスキーを登録することができます。

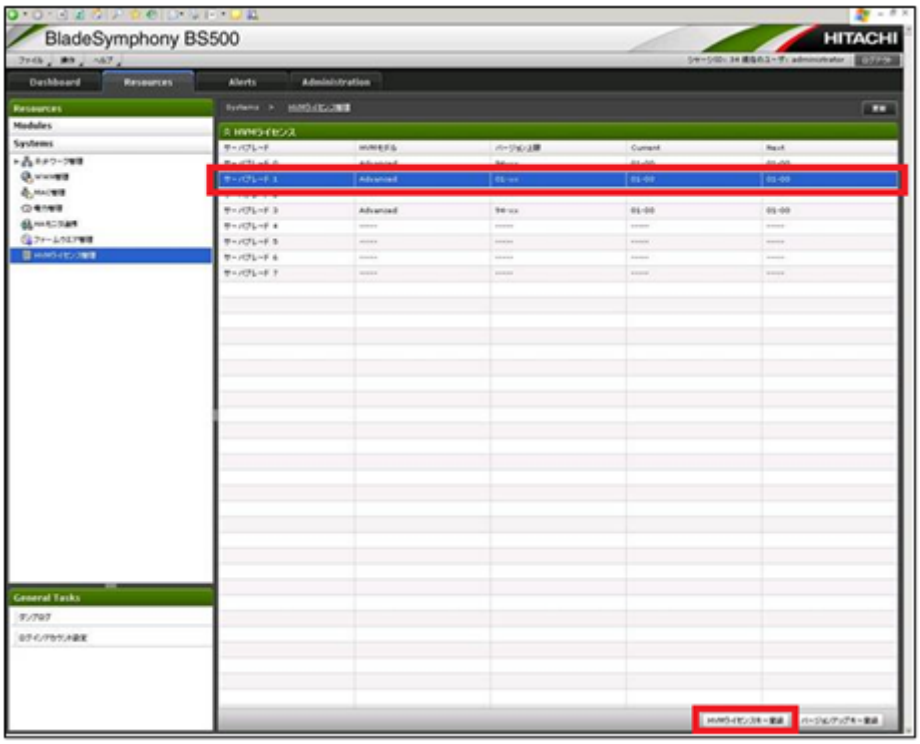
1. [Resources]タブをクリックします。



2. [Resources]パネルの[Systems]アコーディオン内のツリービューから「HVM ライセンス管理」を選択します。



3. [HVM ライセンス]パネルでサーバブレードを選択し，「HVM ライセンスキー登録」ボタンをクリックします。



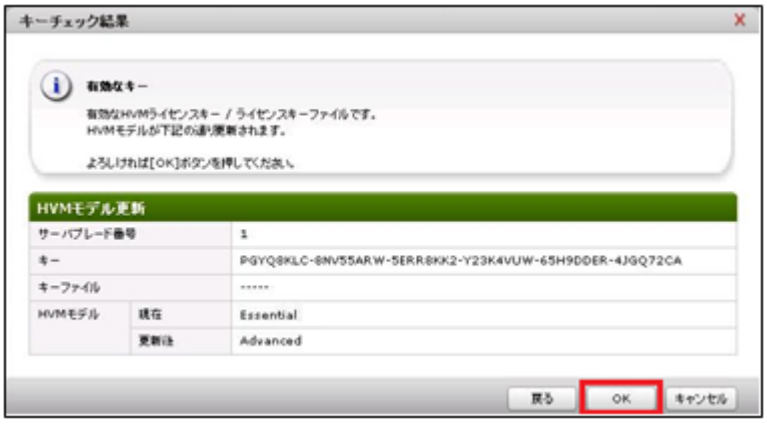
4. ライセンスキーを入力します。
   ライセンスキーの入力方法には，次の 2 通りがあります。

   - HVM ライセンスキーを直接入力する方法
   - HVM ライセンスキーファイルを読み込ませる方法

   HVM ライセンスキーを直接入力する方法

   a. [キー］の［直接入力]ラジオボタンを選択した後，テキストボックスにライセンスキーを入力し，[確認]ボタンをクリックします。

   b. [OK］ボタンをクリックします。



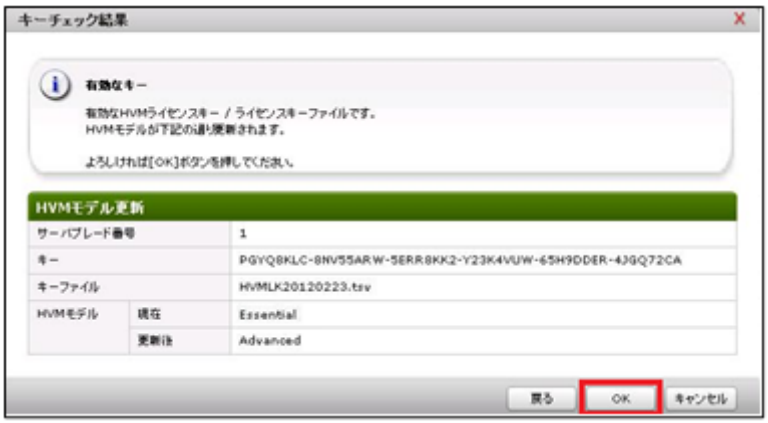
HVM ライセンスキーファイルを読み込ませる方法

a. [ファイル名:]ラジオボタンを選択し，[参照]ボタンをクリックします。

参考 ファイルを開く手順については，OS の操作手順に従ってください。

b. [確認]ボタンをクリックします。

c. [OK]ボタンをクリックします。



2.19.22 HVM ファームウェアのアップデート

HVM ファームウェアバージョンは VV-RR 形式で示されます。バージョンアップは，VV が更新される場合のことを指します。（例：01-00 から 02-00 への更新など）リビジョンアップは，RR が更新される場合のことを指します。（例：01-00 から 01-01 への更新など）

HVM ファームウェアをバージョンアップするためには，バージョンアップキーを取得し，Web コンソールでそのバージョンアップキーを HVM に適用する必要があります。

HVM ファームウェアは，マネジメントモジュールの 4 つの格納領域（面）に，4 つの異なったバージョンを格納できます。各サーバブレードは，マネジメントモジュールにインストールされた HVM ファームウェアのうち，どの面のバージョンを使うかを選択できます。

HVM ファームウェアは，インストールとアンインストールの操作ができます。既にインストールされている面のファームウェアをアップデートする際も，インストールにより実施します。

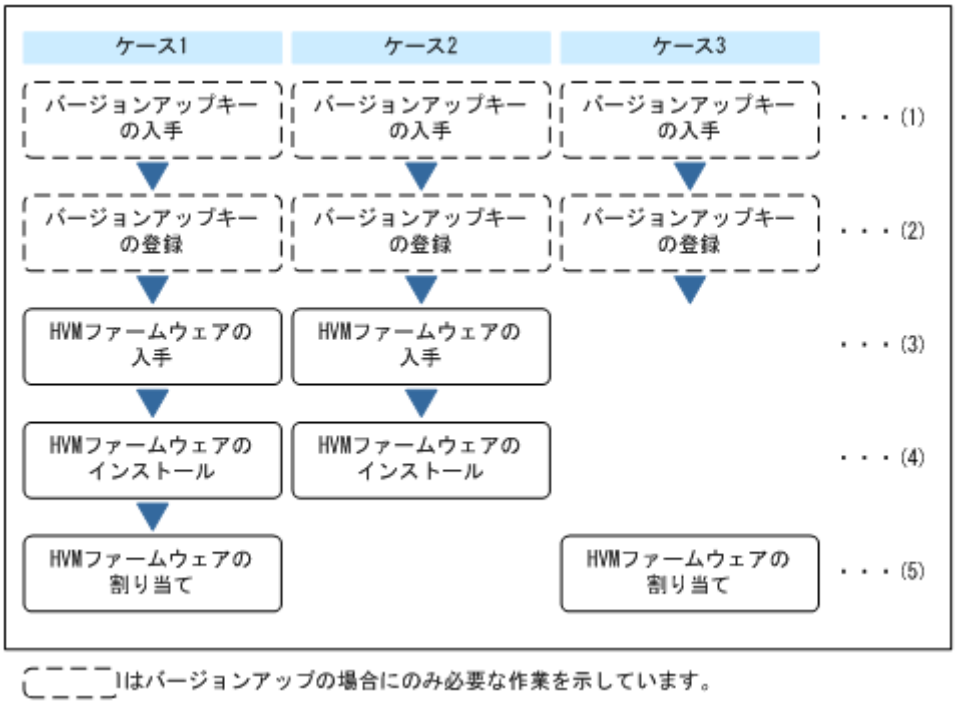
HVM 稼働中に HVM ファームウェアのインストール，および HVM ファームウェアの割り当てが可能であり，HVM 再起動後に新しい HVM ファームウェアにアップデートされます。

HVM ファームウェアのアップデートには，約 10～15 分かかります。

アップデート後は必ずバージョンを確認し，期待するバージョンが表示されていることを確認してください。

HVM ファームウェアのアップデート手順は次のとおりです。

項目	内容
ケース 1	当該サーバブレードに割り当てられていない面に対して，HVM ファームウェアをインストールする場合
ケース 2	当該サーバブレードに割り当てられている面に対して，HVM ファームウェアをインストールする場合
ケース 3	すでにインストールされている面の HVM ファームウェアを利用する場合



重要

- HVM ファームウェアバージョンを 01-4X 以降に更新する場合は，次の拡張カード類の使用有無を確認してください。使用している場合は，ファームウェアの更新が必要な場合があります。

  - Emulex 10Gb CNA/LAN 拡張カード

  - オンボード CNA

- HVM ファームウェアバージョンと拡張カード類のファームウェアバージョンの組み合わせについては，「*BladeSymphony BS500 HVM ユーザーズガイド*」の「注意事項」の章を参照してください。

- Emulex 10Gb CNA/LAN 拡張カード，オンボード CNA のファームウェアバージョンの確認，および更新方法は「BS500 サーバブレードオンボード 10Gb CNA/LAN 及び 10Gb CNA/LAN 拡張カードファームアップ手順書(BladeSymphony FW Update Tool 操作説明書)」を参照してください。

  手順書は，上記の拡張カード類のファームウェアに同梱されていますので，BladeSymphony ホームページから入手してください。なお，ファームウェアの入手方法は「(3) HVM ファームウェアの入手」を参照してください。

参考

- マネジメントモジュールを非冗長構成で使用されている場合，マネジメントモジュールが故障して保守交換すると HVM ファームウェアが消失するため，再インストールが必要になります。冗長構成で使用することを推奨します。

- HVM ファームウェアをマネジメントモジュールにインストールしただけでは，HVM は使用できません。サーバブレードで使用する HVM ファームウェアの面を，必ず選択してください。HVM ファームウェアの面の選択は，マネジメントモジュールのコンソールから実施できます。
- HVM ファームウェアのインストール中に，マネジメントモジュールの交替が発生した場合，インストールに失敗します。障害要因を取り除いた後，再実行してください。
- HVM ファームウェアのインストール中は，インストール対象面を選択しているサーバブレードの電源 ON 操作は抑止されます。
- HVM ファームウェアのインストール中は，インストール対象面をサーバブレードに割り当てることはできません。

(1) バージョンアップキーの入手

バージョンアップキーの入手方法について説明します。

【サポートサービスに契約している場合】

サポートサービスのホームページよりご契約者様専用ページにログインし，バージョンアップキーを入手します。

ホームページアドレス:http://www.hitachi-support.com/

詳細については，サポートサービスにお問い合わせください。

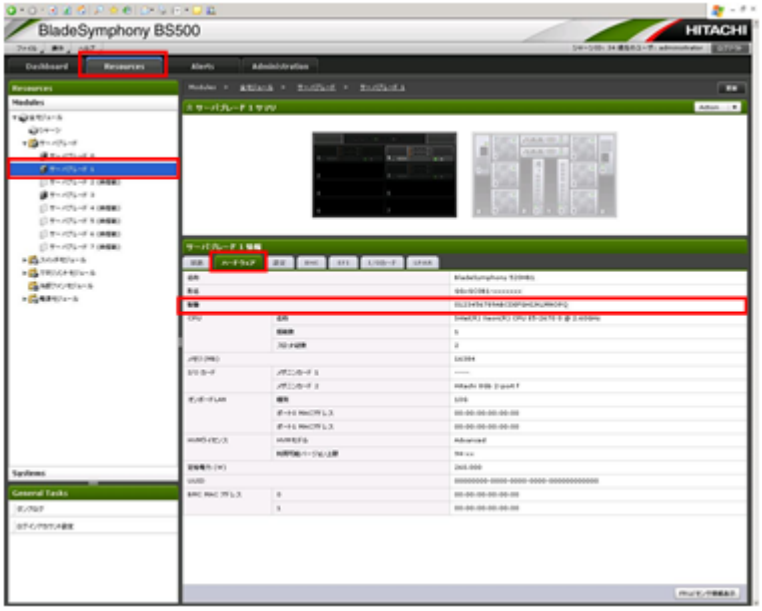
【サポートサービスに契約していない場合】

次のものを用意する必要があります。

- WAK（Web Access Key）
  弊社営業に問い合わせの上，Virtage バージョンアップライセンスをご購入ください。
- ブレードシリアル番号
  Web コンソールで対象サーバブレードのブレードシリアル番号を確認してください。

参考

- ここでは，サーバブレードの製番をブレードシリアル番号と呼びます。
- サーバブレードの製番は次の手順で確認できます。
  [Resources]タブ－[Resources]パネル－[Modules]アコーディオン内のツリービューからサーバブレードを選択後，[サーバブレード情報]パネルで[ハードウェア]タブを選択すると，製番を表示します。



バージョンアップキーの入手方法

BladeSymphony ホームページよりバージョンアップキー発行画面に移動し，バージョンアップキーを入手します。

ホームページアドレス：http://www.hitachi.co.jp/products/bladesymphony/

1. BladeSymphony ホームページよりバージョンアップキー発行画面に移動します。次のように移動してください。

   [ダウンロード]

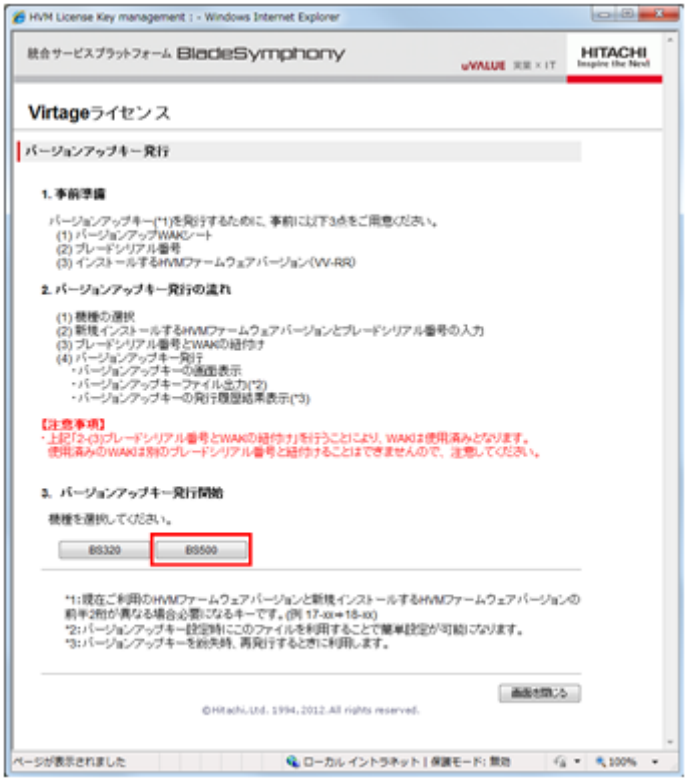
   ↓

   [ライセンスキー]の[詳細はこちら]

   ↓

   [バージョンアップキー]

2. バージョンアップキー発行画面で[BS500]ボタンをクリックします。



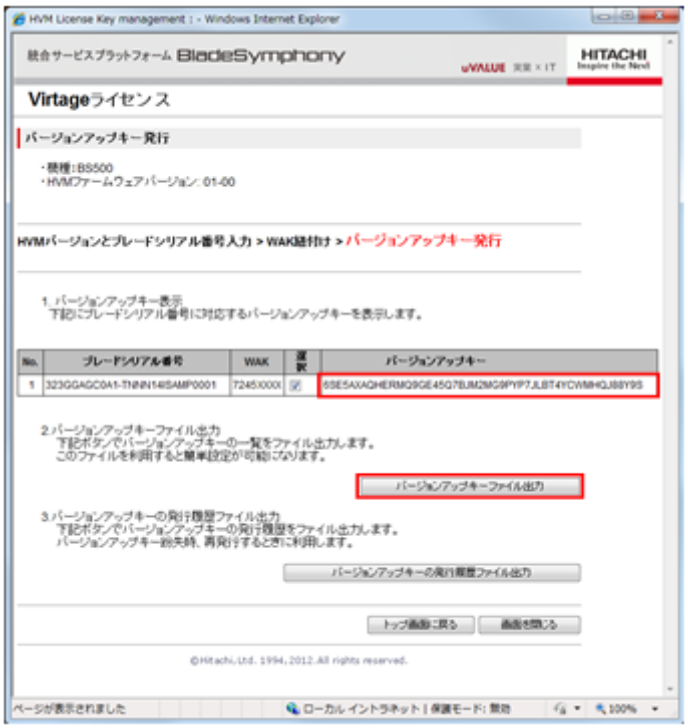
3. ブレードシリアル番号を入力し，[WAK 紐付け画面へ]ボタンをクリックします。

4. WAK を入力し，[バージョンアップキー発行画面へ]ボタンをクリックします。

5. バージョンアップキーを入手します。

「(2) バージョンアップキーの登録」でバージョンアップキーを直接入力する場合は，バージョンアップキーを控えておきます。

「(2) バージョンアップキーの登録」でバージョンアップキーファイルを読み込ませる場合は，[バージョンアップキーファイル出力]ボタンをクリックし，バージョンアップキーファイルをシステムコンソールのハードディスクに格納します。

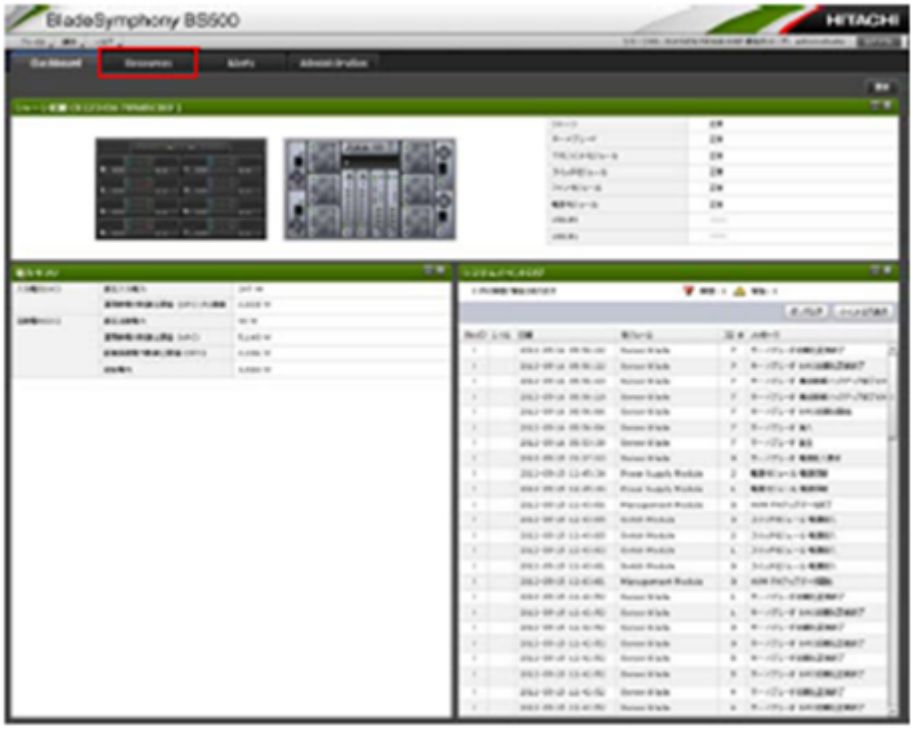


参考 バージョンアップキーファイルを再発行する際は，発行履歴ファイルに記録されたブレードシリアル番号と紐付け済み WAK を，発行時と同様の手順で入力してください。

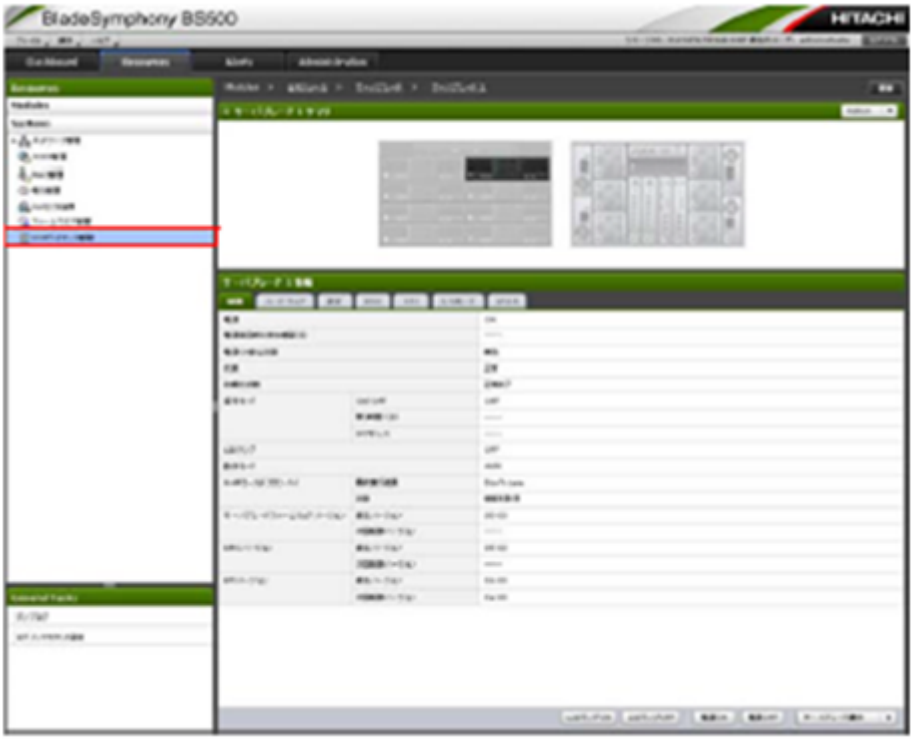
(2) バージョンアップキーの登録

バージョンアップキーの登録方法について説明します。

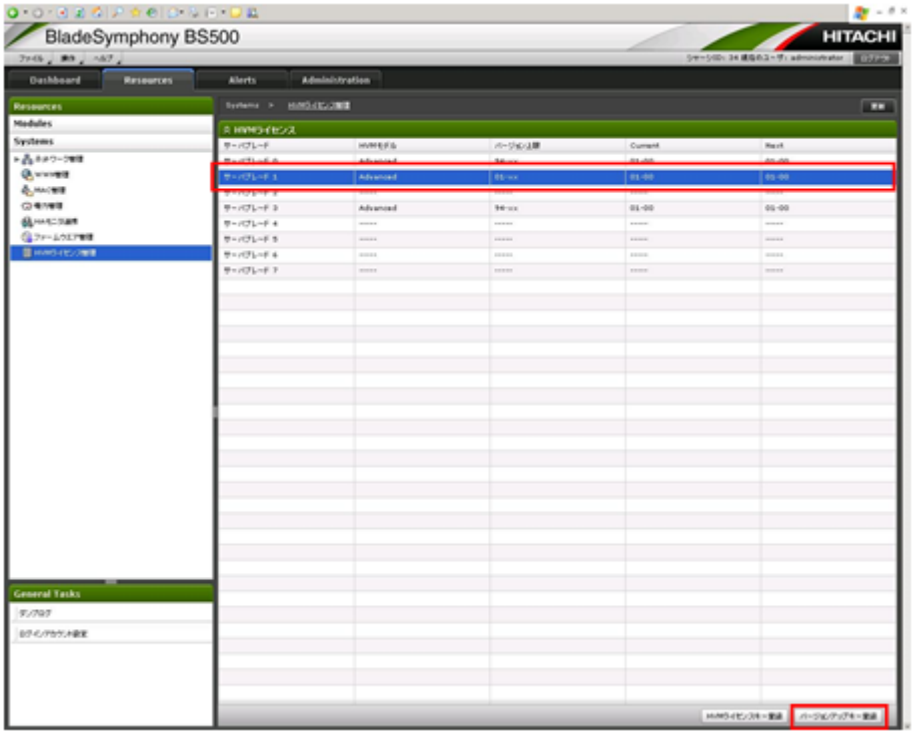
1. [Resources]タブをクリックします。



2. [Resources]パネルの[Systems]アコーディオン内のツリービューから「HVM ライセンス管理」を選択します。



3. [HVM ライセンス]パネルでサーバブレードを選択し，「バージョンアップキー登録」ボタンをクリックします。

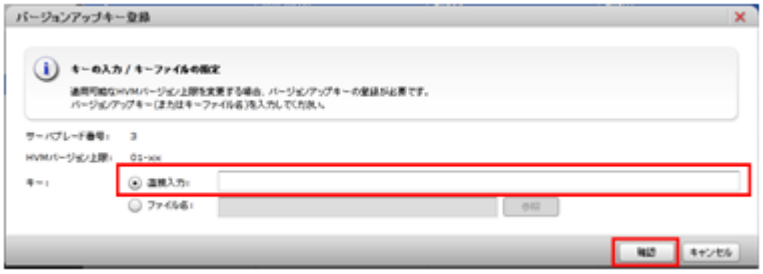


4. バージョンアップキーを入力します。
   バージョンアップキーの入力方法には，次の 2 通りがあります。

   - バージョンアップキーを直接入力する方法
   - バージョンアップキーファイルを読み込ませる方法

   バージョンアップキーを直接入力する方法

a. [キー]の［直接入力]ラジオボタンを選択した後，テキストボックスにバージョンアップキーを入力し，[確認]ボタンをクリックします。



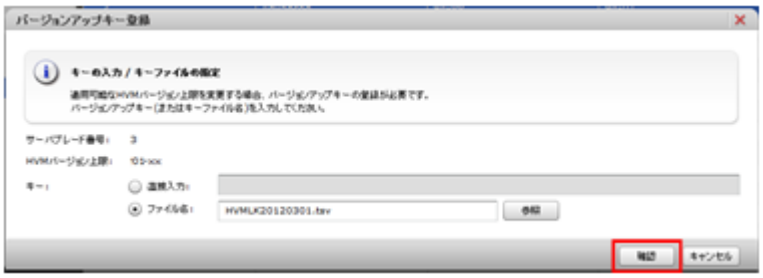
b. [OK]ボタンをクリックします。

バージョンアップキーファイルを読み込ませる方法

a. [ファイル名:]ラジオボタンを選択し，[参照]ボタンをクリックします。

参考 ファイルを開く手順については，OS 操作手順に従ってください。

b. [確認]ボタンをクリックします。



c. [OK]ボタンをクリックします。

(3) HVM ファームウェアの入手

HVM ファームウェアを BladeSymphony ホームページからダウンロードしてください。その後，HVM ファームウェアをシステムコンソールのハードディスクなどに格納してください。

ホームページアドレス:http://www.hitachi.co.jp/products/bladesymphony/

次のとおりに進むことで，HVM ファームウェアの掲載ページを表示することができます。

[ダウンロード]

↓

[ドライバ・ユーティリティ　ダウンロード]の[詳細はこちら]

重要

- ファームウェアファイル名は変更しないでください。変更すると，マネジメントモジュールは，ファームウェアファイルとして認識できません。
- 別機種(例：BS2000)のファイルは適用できません。

参考 キーワードは『Virtage』で検索してください。

(4) HVM ファームウェアのインストール

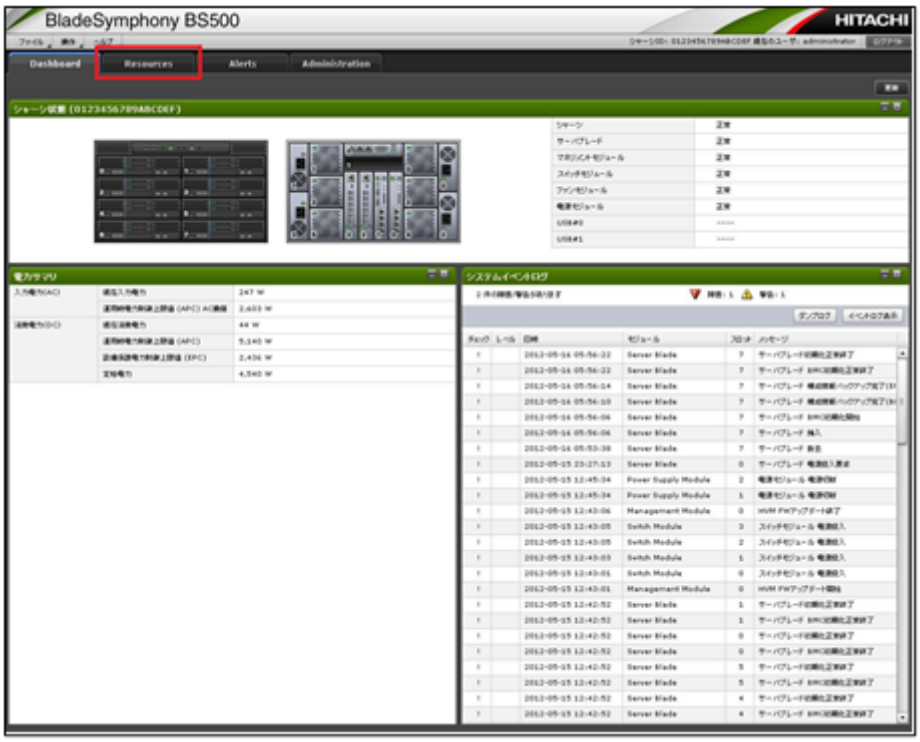
【マネジメントモジュールファームウェアバージョン A0135 以前】

HVM ファームウェアは，サーバブレードに割り当てられていない面に対してのみインストールすることができます。

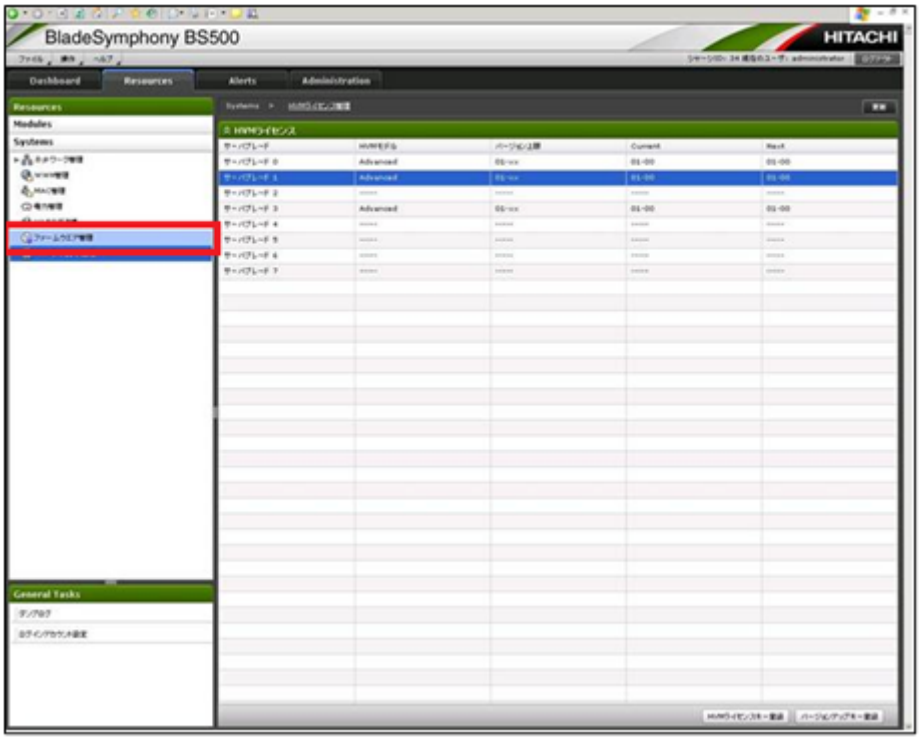
【マネジメントモジュールファームウェアバージョン A0145 以降】

HVM ファームウェアは，サーバブレードに割り当てられていない面，または割り当てられている全てのサーバブレードの電源が OFF となっている面に対してのみインストールすることができます。

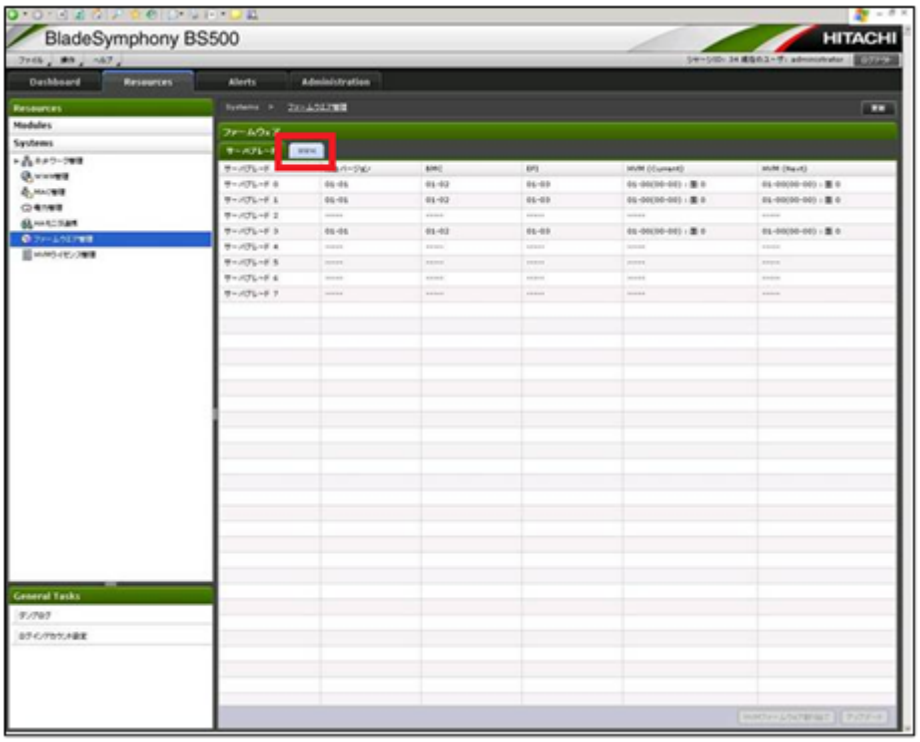
1. [Resources]タブをクリックします。



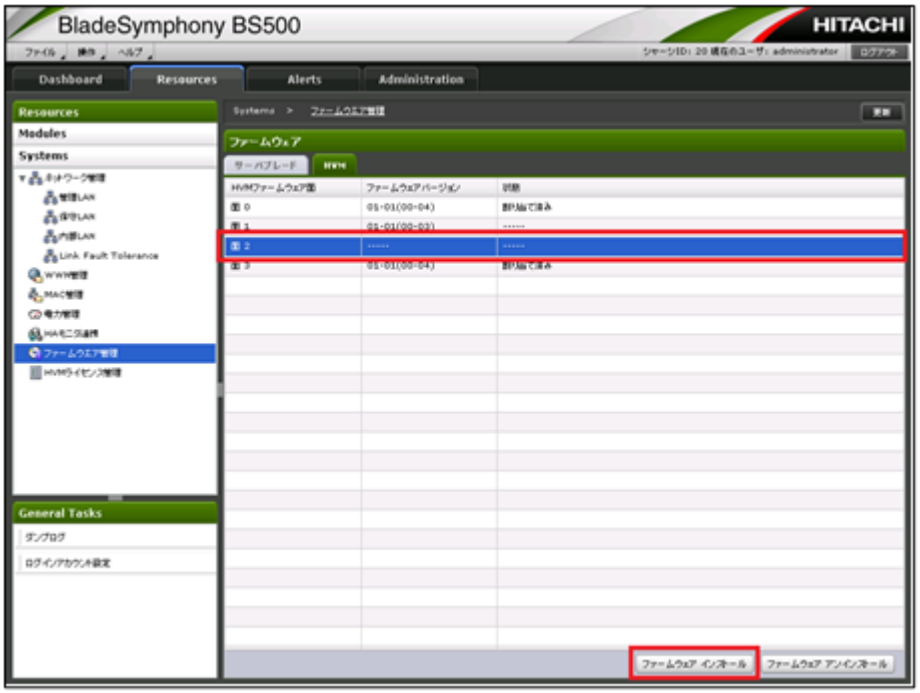
2. [Resources]パネルの[Systems]アコーディオン内のツリービューから「ファームウェア管理」を選択します。



3. 「HVM」タブを選択します。



4. 「ファームウェア」パネルで面を選択し,「ファームウェアインストール」ボタンをクリックします。



5. 「参照」ボタンをクリックします。

参考 ファイルを開く手順については，OS の操作手順に従ってください。

6. 「確認」ボタンをクリックします。

7. 選択した面の状態によって，手順が異なります。

   - 手順 4 で[状態]が「-----」となっている面を選択した場合

     手順 9 へ進んでください。

   - 手順 4 で[状態]が「割り当て済み(ファームウェア上書き可能)」となっている面を選択した場合

     [バックアップ対象サーバブレード]パネルで構成情報のバックアップを行うサーバブレードを選択し，[バックアップ]ボタンをクリックします。

8. [保存]ボタンをクリックします。

参考

- バックアップ対象として選択したサーバブレードと同じ個数のファイルがダウンロードされます。
- ファイルの保存手順については，OS の操作手順に従ってください。
- ファイル名称は次のようになります。

  hvm-pX-VVRR-YYYYMMDDhhmmss.backup

  ここで，X はパーティション(サーバブレード)番号，VVRR は現在割り当てられている HVM バージョンが入ります。

9. 「OK」ボタンをクリックします。

参考 「構成情報のバックアップ」「実行済み」「未実行」は，インストール先に「割り当て済み(ファームウェア上書き可能)」となっている面を選択した場合にのみ表示されます。
【マネジメントモジュールファームウェアバージョン A0145 以降】

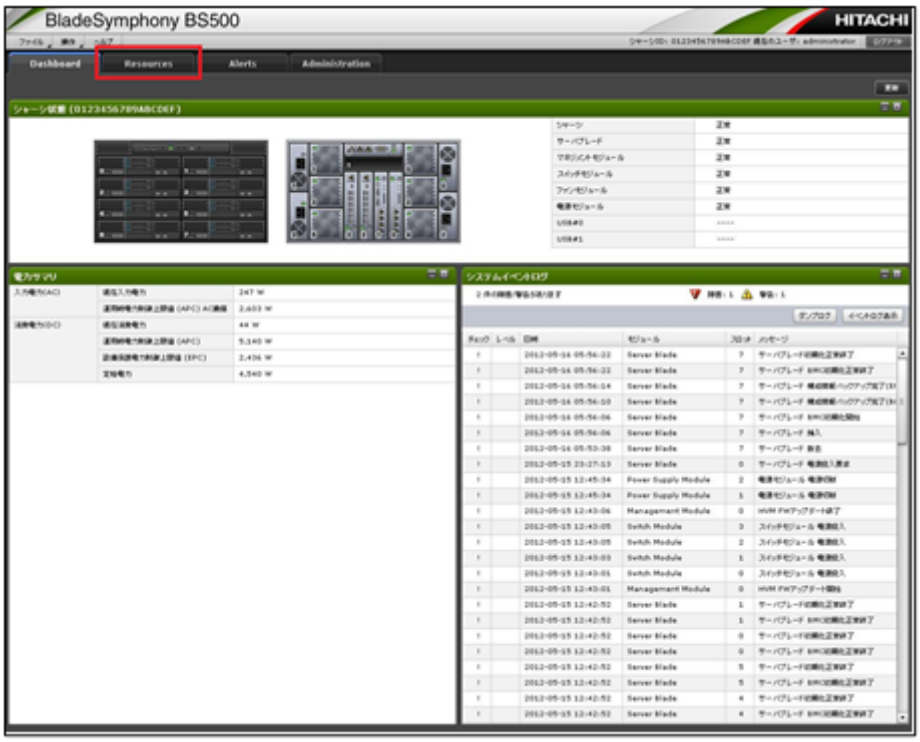
10. 「閉じる」ボタンをクリックします。

(5) HVM ファームウェアの割り当て

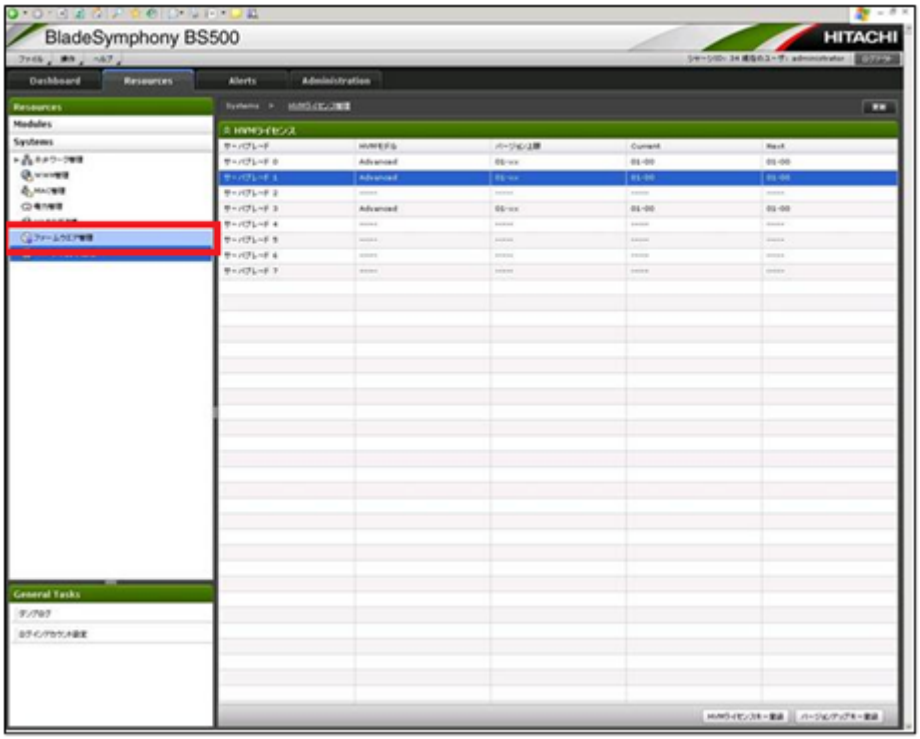
HVM ファームウェアの割り当て手順を説明します。

参考 SMP 構成の場合は，プライマリサーバブレードにファームウェアを割り当ててください。

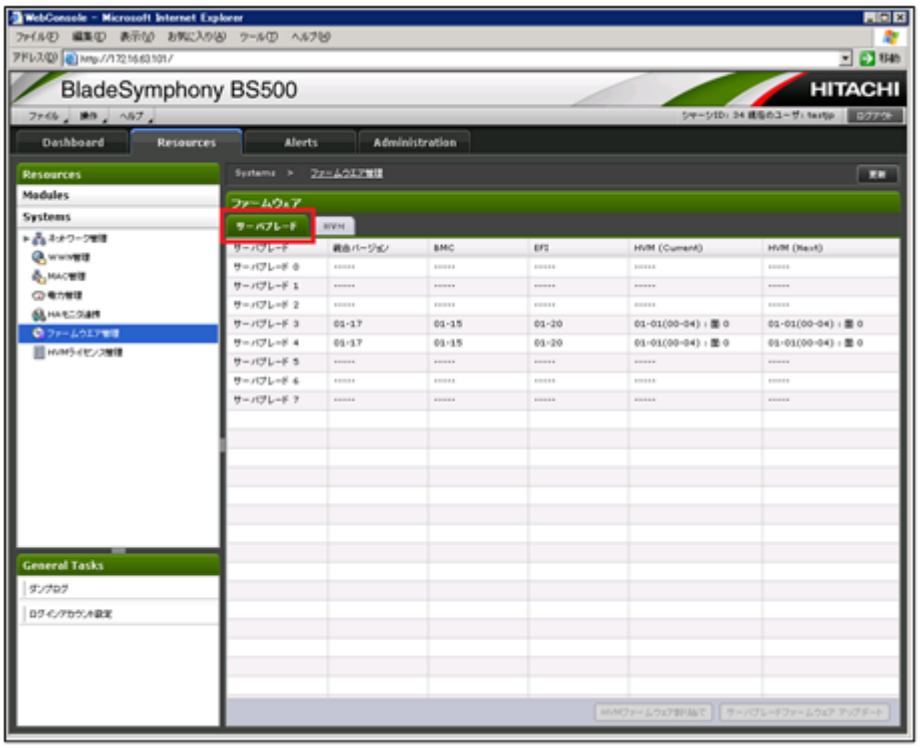
1. [Resources]タブをクリックします。



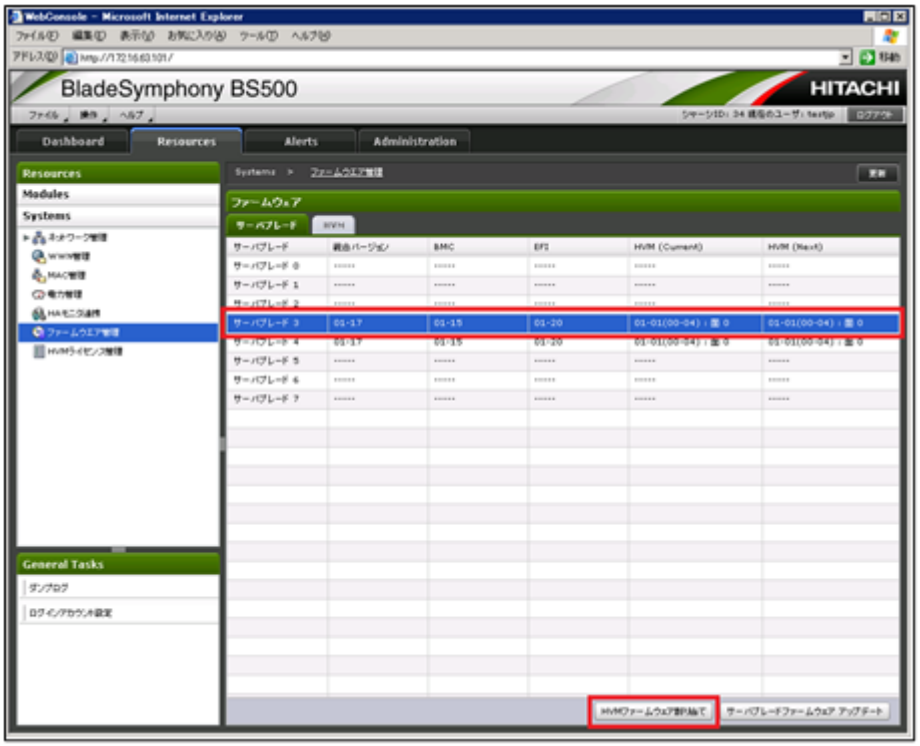
2. [Resources]パネルの[Systems]アコーディオン内のツリービューから「ファームウェア管理」を選択します。



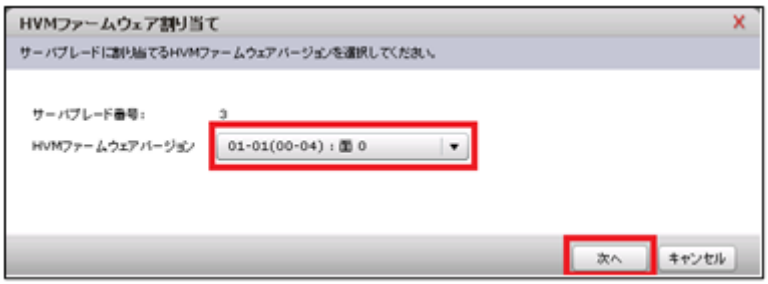
3. 「サーバブレード」タブを選択します。



4. 割り当てするサーバブレードを選択し，「HVM ファームウェア割り当て」ボタンをクリックします。



5. 「HVM ファームウェアバージョン」コンボボックスから面を選択し，「次へ」ボタンをクリックします。



6. 「バックアップ」ボタンをクリックします。

   HVM ファームウェアのインストール時に構成情報のバックアップを行っている場合は，手順８へ進んでください。

7. 「保存」ボタンをクリックします。

参考 ファイルの保存手順については，OS の操作手順に従ってください。

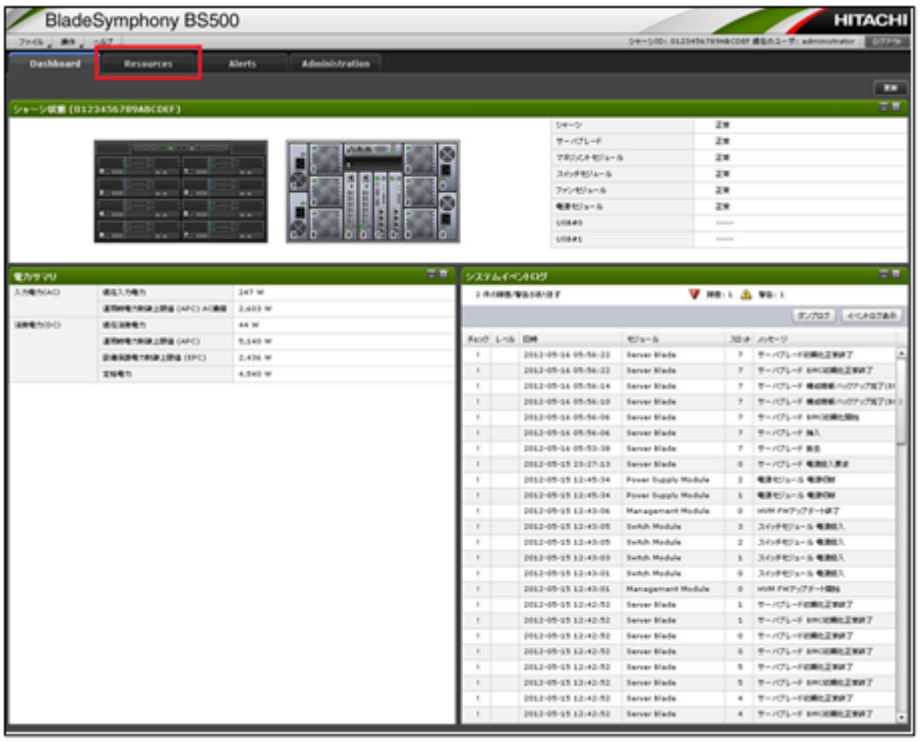
8. 「確認」ボタンをクリックします。

9. 「OK」ボタンをクリックします。

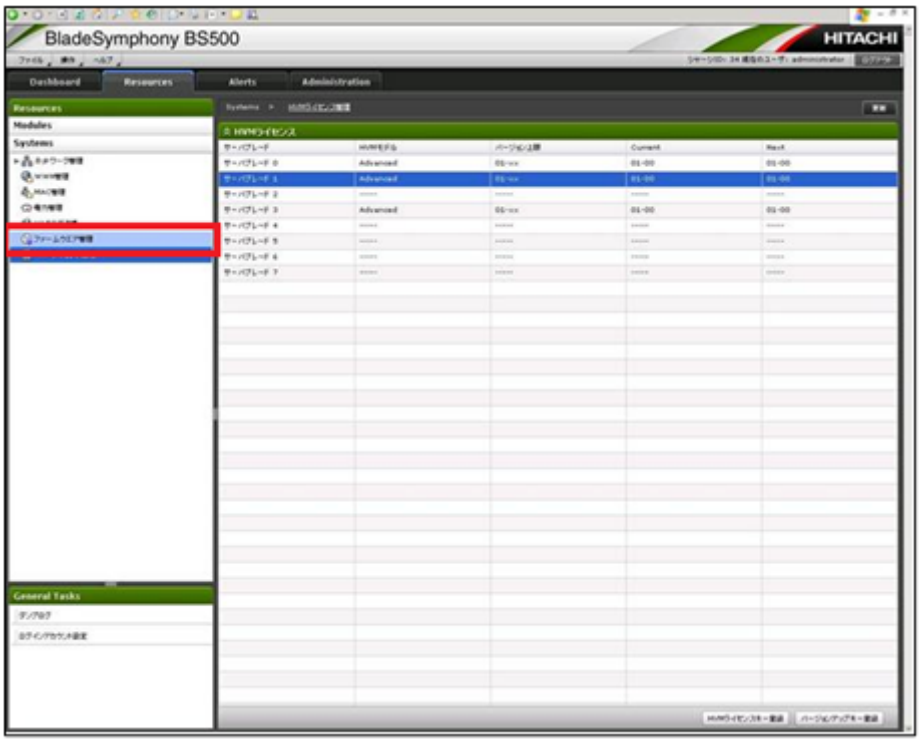
2.19.23 HVM ファームウェアのアンインストール

HVM ファームウェアのアンインストールは，サーバブレードに割り当てられていない面に対してのみ実施できます。

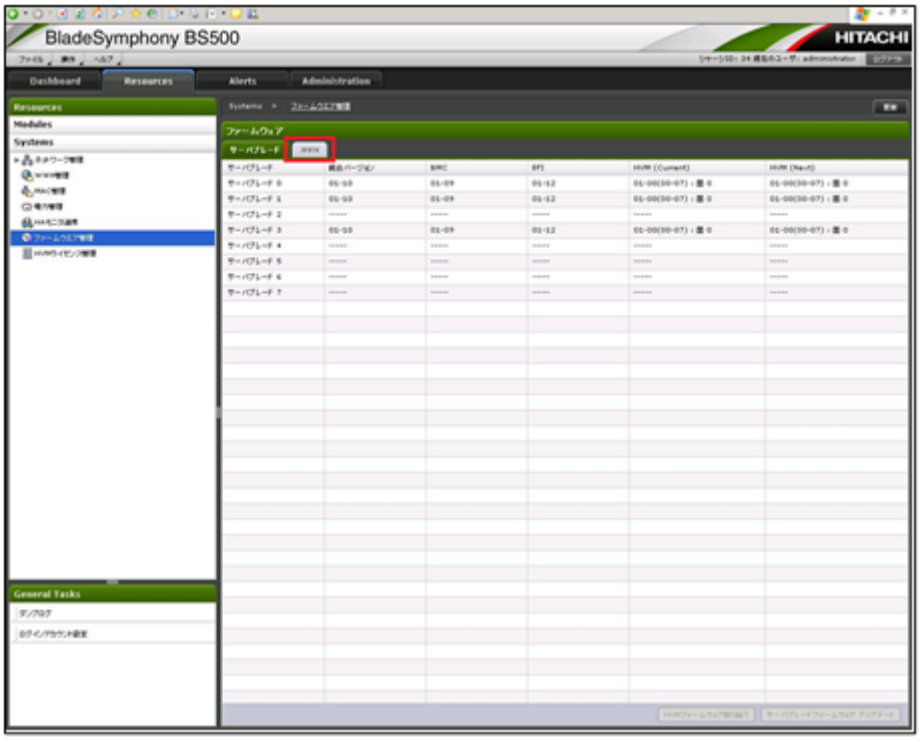
1. [Resources]タブをクリックします。



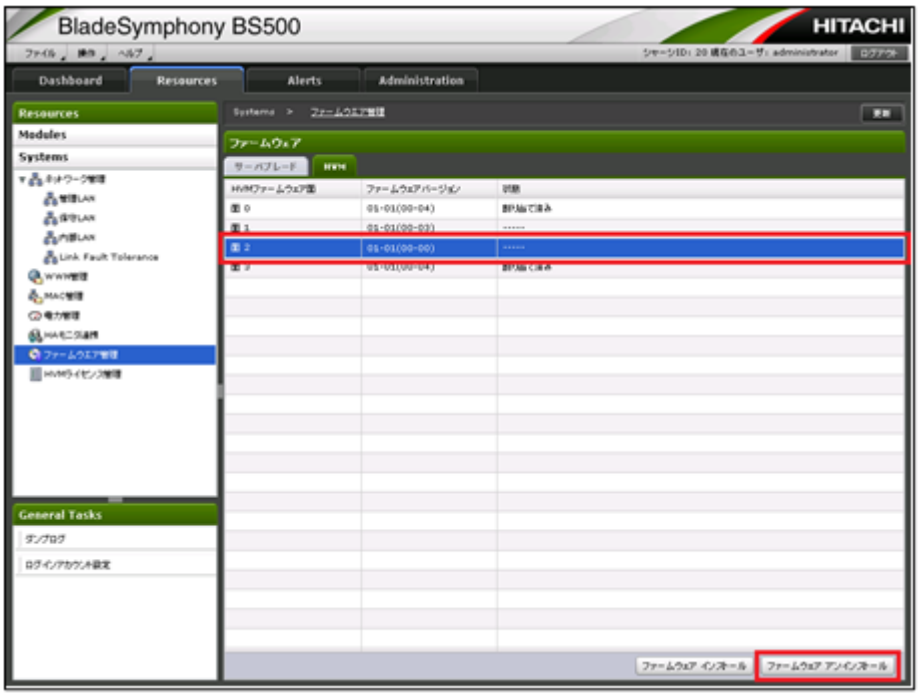
2. [Resources]パネルの[Systems]アコーディオン内のツリービューから「ファームウェア管理」を選択します。



3. 「HVM」タブを選択します。



4. 「ファームウェア」パネルで面を選択し，「ファームウェア アンインストール」ボタンをクリックします。



5. 「OK」ボタンをクリックします。

6. 「閉じる」ボタンをクリックします。

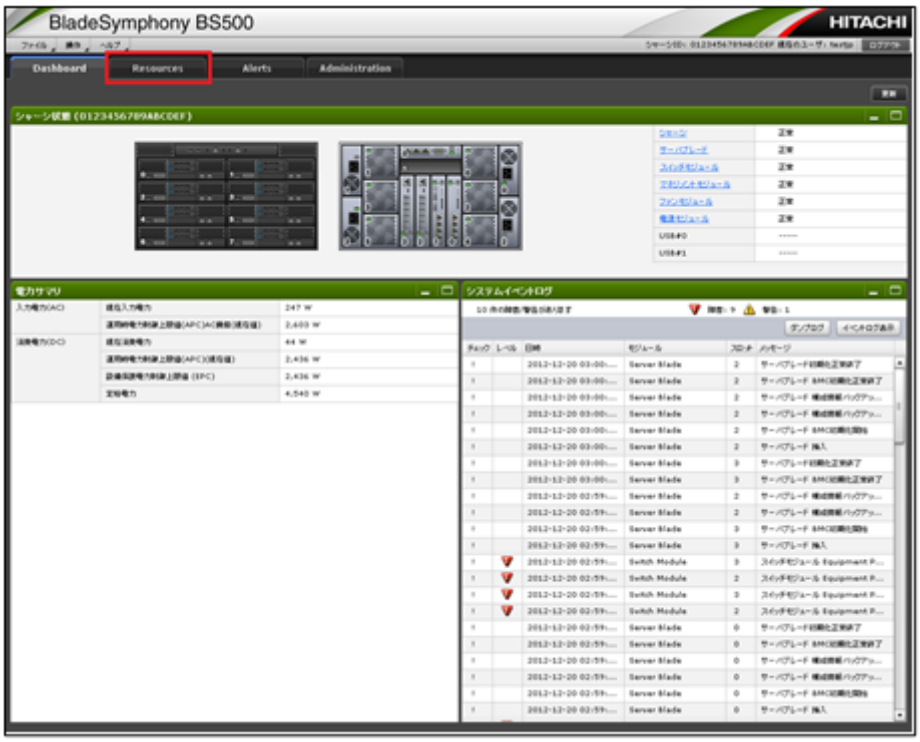
2.19.24 HVM 稼働時ダンプの採取

HVM 稼働時ダンプを採取する手順を説明します。

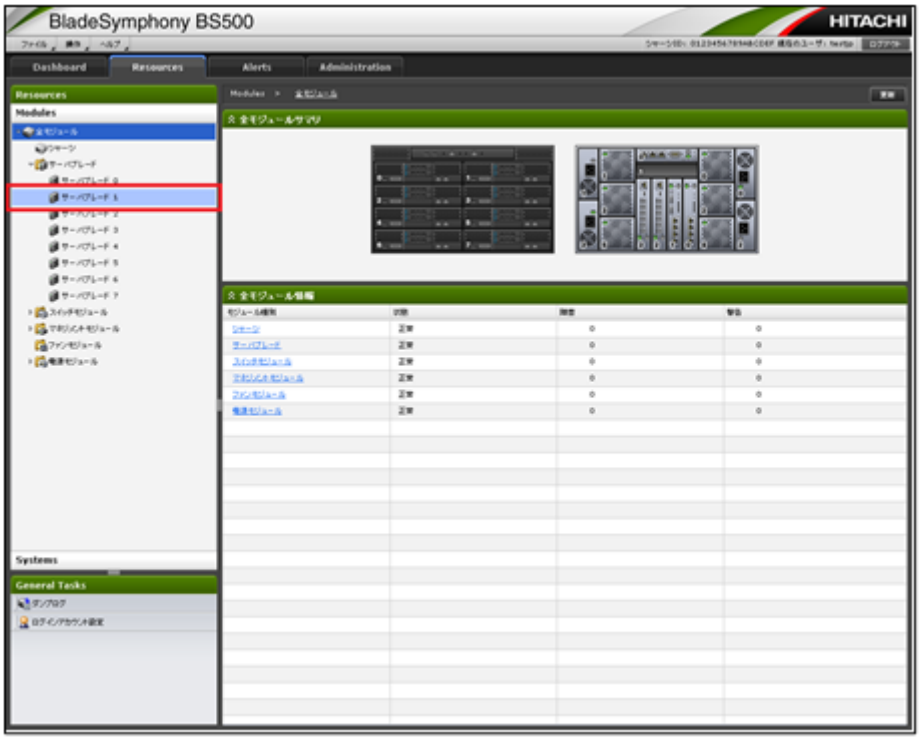
この操作により採取する HVM ダンプは，障害が発生した場合の障害解析に使用します。通常の運用では HVM ダンプを採取する必要はありません。装置に異常がみられる場合に HVM ダンプを採取していただく場合があります。

【マネジメントモジュールファームウェアバージョン A0145 以降】

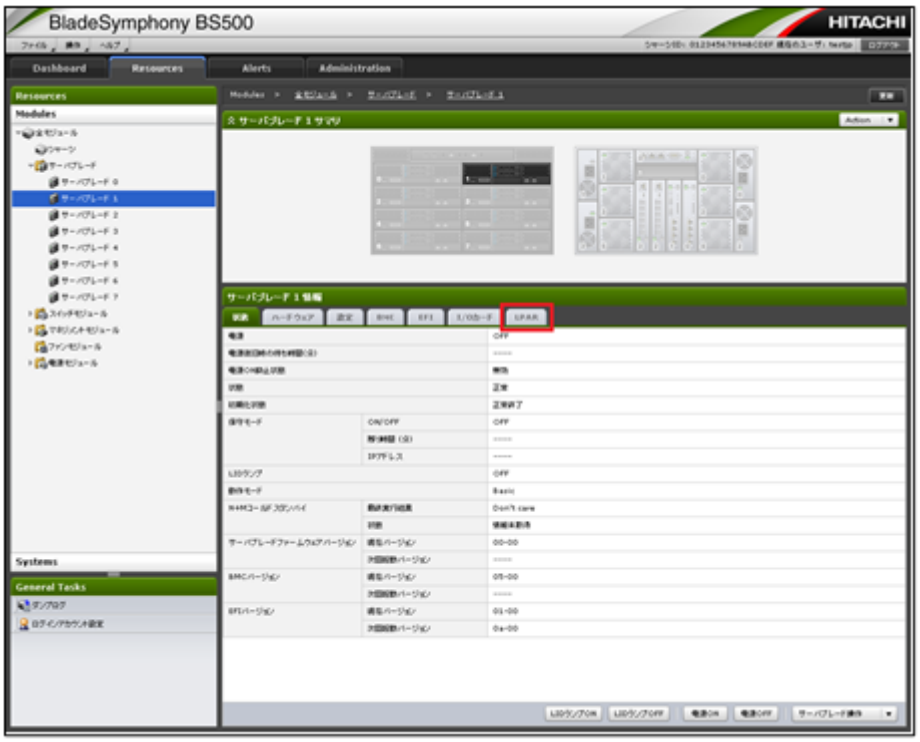
1. [Resources]タブをクリックします。



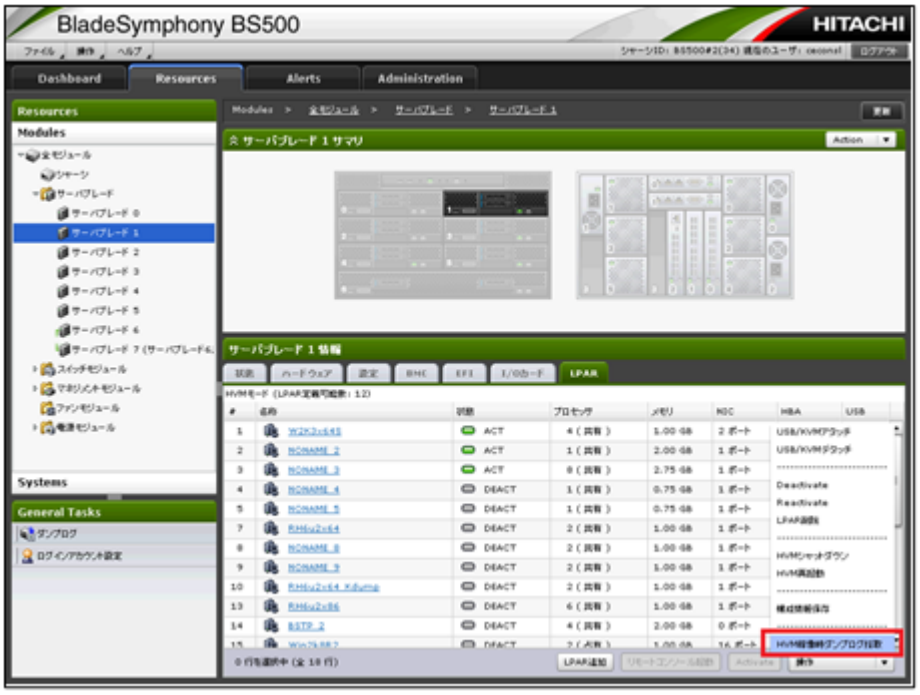
2. [Resources]パネルの[Modules]アコーディオン内のツリービューからサーバブレードを選択します。



3. [サーバブレード]パネルの[LPAR]タブを選択します。



4. [LPAR]タブにある[操作]メニュー内の[HVM 稼働時ダンプログ採取]をクリックします。



5. [OK]ボタンをクリックします。処理が完了するとファイルとしてダウンロードされます。

参考

- ファイルの保存手順については，OS の操作手順に従ってください。
- 本手順により採取する HVM 稼働時ダンプログは，ファイルとしてダウンロードすることができますが，マネジメントモジュールには保存されません。

2.20 省電力機能

システム装置の省電力機能について説明します。

2.20.1 電力制限機能の管理

システム装置では設備保護電力制御（EPC）機能，運用時電力制御（APC）機能および DCMI を提供します。EPC 機能および APC 機能の設定可能範囲は，電源構成設定，および運用時電力制御設定に基づき，マネジメントモジュールで自動計算されます。

電力制限機能に関連する設定項目を次の表に示します。これらは，DCMI モードの有効/無効を切り替える設定を除き，サーバブレードの電源 ON 状態時にも設定を変更できます。ただし，その場合は，サーバブレードの継続稼働を優先するようマネジメントモジュール側で自動的に設定可能範囲を制限します。

表 2-102 電力制限機能に関連する設定項目

項目			内容
電源構成設定	電源モジュール冗長構成		システム装置の電源モジュール冗長構成を設定します。 ・ 100VAC：N+N/N+1(デフォルト)/N+0 ・ 200VAC-240VAC：N+N/N+1(デフォルト) 本設定に基づき，システム装置で使用可能な電力をマネジメントモジュールで自動計算します。
	電源容量拡張機能		電源容量拡張機能の有効/無効を設定します。 ・ 無効/有効(デフォルト) 本設定に基づき，システム装置で使用可能な電力をマネジメントモジュールで自動計算します。
設備保護電力制御設定(EPC)	電源設備環境設定(Facility Capping)	有効/無効設定	設備保護電力制御(EPC)に対する電源設備環境(Facility Capping)の有効/無効を設定します。 ・ 無効(デフォルト)/有効 本設定が無効の場合，システム装置内蔵の電源モジュール定格に基づき，システム装置で使用可能な電力をマネジメントモジュールで自動計算します。 本設定が有効の場合，システム装置内蔵の電源モジュール定格および電源設備環境設定に基づき，システム装置で使用可能な電力をマネジメントモジュールで自動計算します。
		サーキットブレーカ定格電流	設備のサーキットブレーカ定格電流を設定します。 ・ 100VAC：10A-100A (デフォルト=15A) ・ 200VAC-240VAC：15A-100A (PDU 数量=0 のとき，デフォルト=15A。PDU 数量≧1 のとき，デフォルト=30A)
		サーキットブレーカ台数	設備のサーキットブレーカ台数を設定します。 ・ 1/2/3/4 (N+N のとき，デフォルト=2。N+1 のとき，デフォルト=1。N+0 のとき，デフォルト=1)
		PDU 定格電流	PDU 入力定格電流を設定します。 ・ 100VAC：非サポート

項目			内容
			• 200VAC-240VAC：15A-100A(デフォルト=24A)
		PDU 台数	PDU 台数を設定します。 • 0/1/2 (N+N のとき，デフォルト=2。N+1 のとき，デフォルト=1。ただし，電源モジュール 4 台構成時は，電源モジュール冗長構成によらずデフォルト=2)
	サーバブレードの設備保護電力制御(EPC)有効/無効設定		パワーキャッピング(電力制限)の対象としたいサーバブレードを選択できます。 • 無効/有効(デフォルト) 本設定は無効に設定しないでください。
運用時電力制御設定(APC)	運用時電力制御上限設定		装置の運用時の電力上限値を設定します。 システム装置の最大供給電力からシステム装置の最小消費電力の範囲を超えて設定することはできません。 出荷時の設定値は，システム装置の最大供給電力です。 システム装置の最小消費電力は，各搭載モジュールの定格電力の合計値に対し，サーバブレードの運用時電力制御(APC)有効/無効設定が有効であるサーバブレードについて，最もパワーキャッピングをかけたときの最大消費電力を適用した値です。
	サーバブレードの運用時電力制御(APC)有効/無効設定		パワーキャッピング(電力制限)の対象とするサーバブレードを選択できます。 SMP 構成の場合，プライマリサーバブレードの設定が SMP を構成するすべてのサーバブレードに適用されます。ノンプライマリサーバブレードの設定は不要です。 出荷時の設定は，「有効」です。 本設定を変更すると，システム装置の最小消費電力が変化します。運用時電力制御上限設定の値がシステム装置の最小消費電力を下回ることとなる設定はできません。
Datacenter Management Interface(DCMI)	サーバシャーシ全体の DCMI モード有効/無効設定		サーバシャーシ全体の DCMI モードの有効/無効を設定します。 出荷時の設定は，「無効」です。 DCMI モードの有効/無効の切り替えは，サーバシャーシ内のすべての DCMI 対応サーバブレードの初期化が終了し，かつメイン電源が OFF の場合にだけ行えます。 DCMI モードと APC 機能は排他のため，両方同時に使用することはできません。

参考 電力制限機能は運用時電力制御機能（APC）の使用を推奨します。
DCMI ではマネジメントモジュールを使用したシャーシ全体としての電力制御が行えません。
また，DCMI を使用するにはサーバブレードが DCMI に対応している必要があります。
用途に応じて使用する電力制限機能を選択してください。

重要

- DCMI(2.21 DCMI 機能参照)と APC を同時に有効にすることはできません。DCMI モードを有効にした場合，APC は自動的に無効となり APC に関する設定変更は行えません。
- DCMI モードを有効に設定した場合，APC の設定内容は初期化されます。同様に DCMI モードを無効に設定した場合も，DCMI の設定内容は初期化されます。
- DCMI と EPC は同時に利用することができます。電源障害などにより供給電力が不足する状況となった場合，装置の継続稼働のため EPC によるパワーキャッピングが優先して実行されます。

2.20.2 設備保護電力制御機能

設備保護電力制御(EPC : Emergency Power Control)機能は，高速なサーバブレードのパワーキャッピング(電力制限)により，システム装置内蔵の電源モジュール，および，ご使用の電源設備環境(設

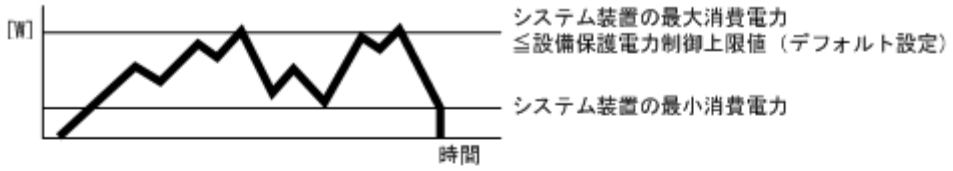
備のサーキットブレーカ，PDU など)を電源設備の電力許容量を超える電力過負荷状態から保護する機能を提供します。

本機能では，電力過負荷状態を検知した場合，サーバブレードの動作周波数をハードウェア制御にて最低レベルまで抑止することで電力制御を実現します。性能抑止状態は約 1 分間継続されます。マネジメントモジュールは，性能抑止解除後約 5 分以内に再び電力過負荷状態を検出すると，再び性能抑止を実施すると同時に，運用時電力制御上限値を，強制的に設備保護電力制御上限値の約 90%以下に再設定してサーバブレードの消費電力を抑止することで，本制御による性能抑止発生をできるだけ低減します。本強制設定は，以後 1 時間，運用時電力制御上限値を超過しなかった場合は自動的に解除されます。また，システム装置の AC オフによっても本強制設定は解除されます。

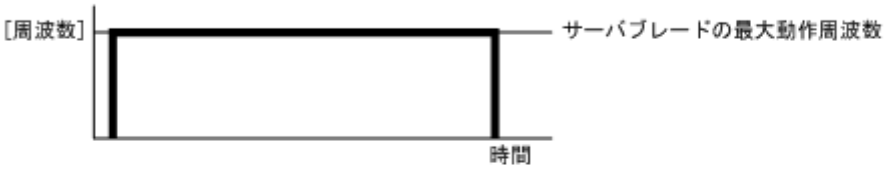
本機能では，使用する電源設備と電源モジュールの定格から，システム装置の消費電力上限値を設定します。

■システム装置の最大消費電力　≦　設備保護電力制御上限値（デフォルト設定）

①システム装置の消費電力

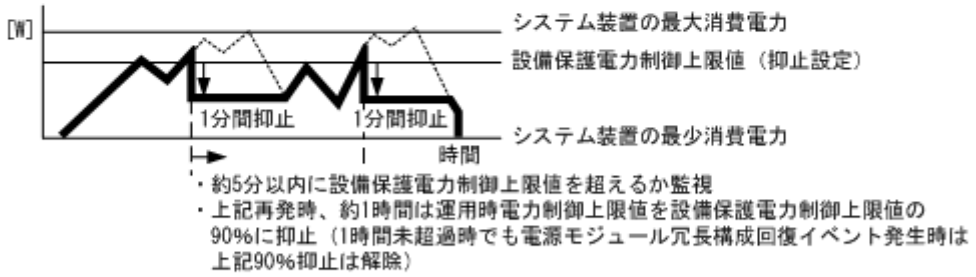


②サーバブレードのCPU動作周波数

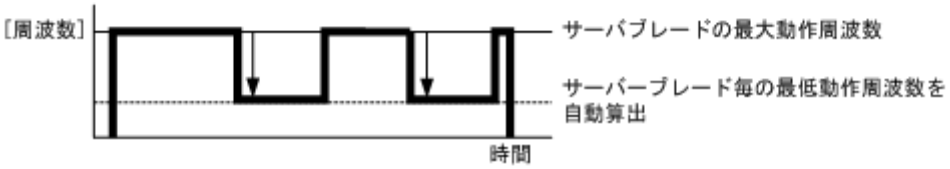


■システム装置の最大消費電力　＞　設備保護電力制御上限値（抑止設定）

①システム装置の消費電力



②サーバブレードのCPU動作周波数



参考

- 電源モジュールが冗長構成の場合は，電源容量拡張機能を有効(デフォルト)に設定することで，設備保護電力制御上限値を大きくすることが可能です。
- 設備保護電力制御上限値は，電源モジュールの電源 ON 状態をリアルタイムで反映します。したがって，不要電源モジュール OFF 機能により，電源 ON 状態の電源モジュール台数が減った場合，一時的に運用時電力制御上限値より上限値が小さく表示されることがあります。運用時電力制御上限値は設定値であり，電源モジュールの電源 ON 状態は反映されません。
- 仮想化環境では，仮想化サーバ上のすべての仮想マシンの性能が一律に劣化するため，仮想化サーバについては，運用時電力制御（APC）の無効設定を推奨します。

表 2-103 Web コンソールでの操作方法

項目	画面
設備保護電力制御(EPC)関連の表示，設定	Resources タブ → Systems → 電力管理 → Action → 電源設備環境設定

表 2-104 CLI コンソールでの操作方法

項目	コマンド
設備保護電力制御(EPC)関連の表示	show power setting
設備保護電力制御(EPC)関連の設定	set power capping

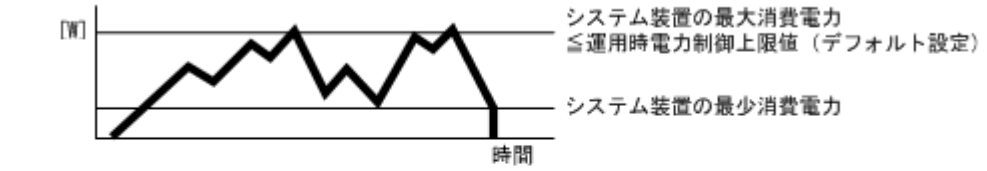
2.20.3 運用時電力制御機能

運用時電力制御(APC：Accurate Power Control)機能は，サーバブレードのパワーキャッピング(電力制限)により，システム装置の運用時電力を運用時電力制御上限値以下に制限する機能を提供します。本機能はソフトウェア制御のため，瞬間的に上限値を上回る場合があります。

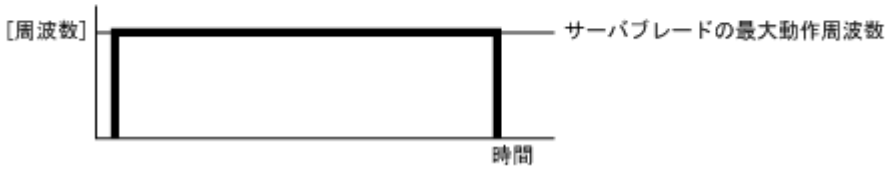
本機能では，運用時電力制御上限値超過を検知した場合，上限値以下になるようサーバブレードの動作周波数を最適レベルまで抑止することで電力制限を実現しています。性能抑止状態は約 1 分間継続されます。なお各サーバブレードの性能抑止の割合は，各サーバブレードのキャッピング能力に対して均一になるよう，マネジメントモジュールが自動計算して割り当てます。

■システム装置の最大消費電力　≦　運用時電力制御上限値（デフォルト設定）

①システム装置の消費電力

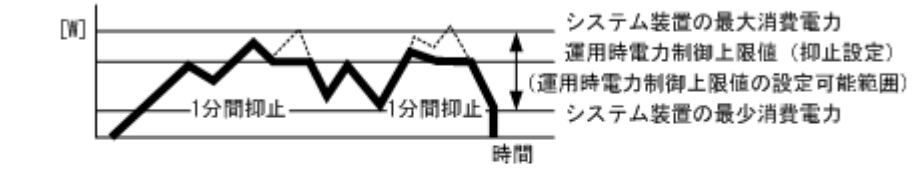


②サーバブレードのCPU動作周波数

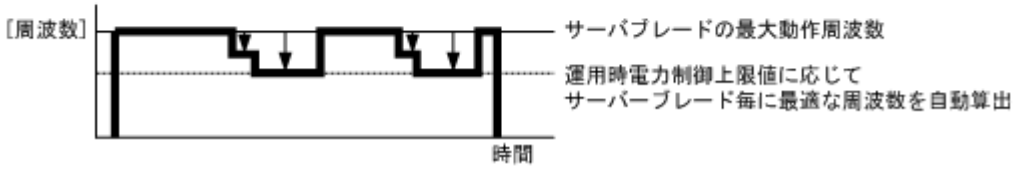


■システム装置の最大消費電力　＞　運用時電力制御上限値（抑止設定）

①システム装置の消費電力



②サーバブレードのCPU動作周波数



参考

- 運用時電力制御上限値に対する一時的な消費電力超過が許容できない場合は，電源設備環境設定により，設備保護電力制御上限値を任意の消費電力に設定してください。

- 一時的な性能抑止が許容できないサーバブレードに対しては，運用時電力制御上限値の設定前に，運用時電力制御(APC)設定を無効にしてください。
- すべてのサーバブレードの一時的な性能劣化が許容できない場合は，運用時電力制御上限値の設定値，サーバブレードに対する運用時電力制御(APC)の有効/無効設定，電源構成設定，電源設備環境設定を見直してください。
- 仮想化環境では，仮想化サーバ上のすべての仮想マシンの性能が一律に劣化するため，仮想化サーバについては，運用時電力制御(APC)の無効設定を推奨します。

表 2-105 Web コンソールでの操作方法

項目	画面
運用時電力制御(APC)関連の表示，設定	Resources タブ → Systems → 電力管理 → Action → 運用時電力上限設定(APC)

表 2-106 CLI コンソールでの操作方法

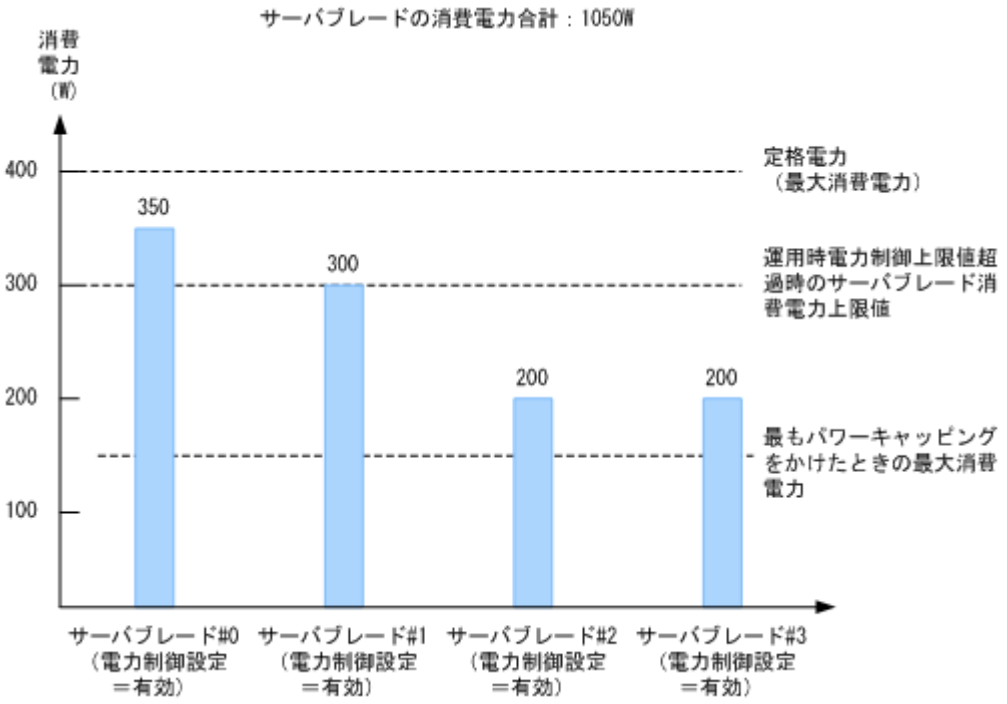
項目	コマンド
運用時電力制御(APC)関連の表示	show power setting
運用時電力制御(APC)関連の設定	set power capping

システム装置の運用時電力上限値が 2000W の場合を例に動作概要を説明します。

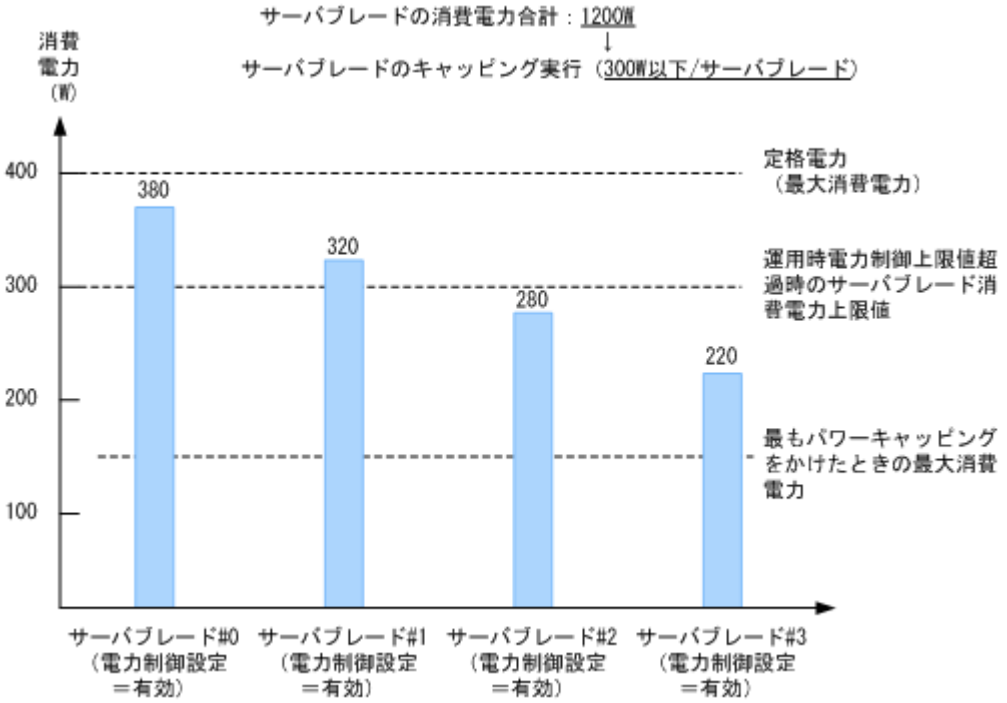
本説明の前提条件は次のとおりです。

- システム装置の運用時電力制御上限値：2000W
- サーバブレード以外の消費電力：800W
  → サーバブレードで使用可能な消費電力：1200W
- サーバブレード消費電力仕様：定格電力(最大消費電力)400W,
  最もパワーキャッピングをかけたときの最大消費電力 150W
- サーバブレード搭載数：4 台(消費電力仕様はすべて同等)
- 運用時電力制御(APC)：有効
  → システム装置の消費電力合計が運用時電力制御上限値超過時はサーバブレード 4 台にてキャッピングがかかり，300W/サーバブレードに電力制限されます。

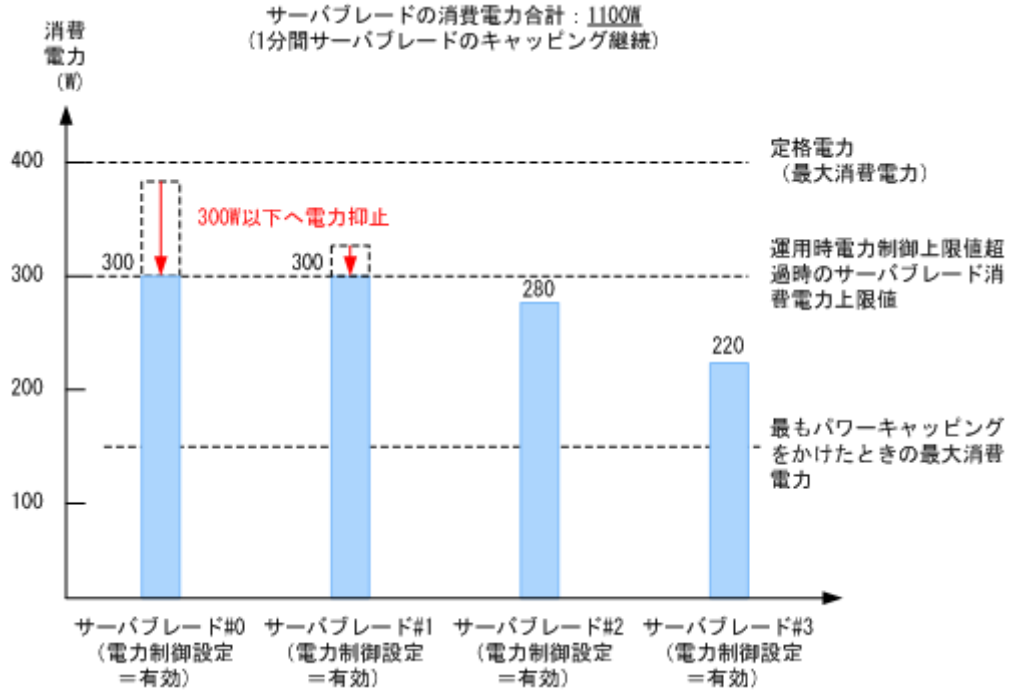
1. 通常運転状態



2. システム装置の消費電力合計が，「運用時電力制御上限値」を超過



3. サーバブレードのキャッピングにより，システム装置の消費電力合計「運用時電力制御上限値」以下へ制御



4. 1 分経過後にキャッピング解除
   →手順 1 に戻る。

2.20.4 サーバブレードに対する電力制御の無効設定

性能抑止が許容できないサーバブレードについては，電力制御の無効設定を行うことで，任意のサーバブレードをキャッピング実行対象外とすることが可能です。

電力制御の無効設定は，設備保護電力制御(EPC)/運用時電力制御(APC)それぞれで設定項目が用意されていますが，設備保護電力制御(EPC)の設定は無効にしないでください。

SMP 構成の場合，プライマリサーバブレードの設定が SMP を構成するすべてのサーバブレードに適用されます。ノンプライマリサーバブレードの設定は不要です。

表 2-107 Web コンソールでの操作方法

項目	画面
サーバブレードに対する電力制御設定の状態表示と設定	Resources タブ → Systems → 電力管理 → サーバブレードタブ → パワーキャッピング設定

表 2-108 CLI コンソールでの操作方法

項目	コマンド
サーバブレードに対する電力制御設定の状態表示	show power setting
設備保護電力制御(EPC)，運用時電力制御(APC)関連の設定	set power capping

例として，システム装置の運用時電力制御上限値が 2000W，サーバブレード 2 台を電力制御を無効に設定した場合の動作概要を説明します。

本説明の前提条件は次のとおりです。

- システム装置の運用時電力制御上限値：2000W
- サーバブレード以外の消費電力：800W
  → サーバブレードで使用可能な消費電力：1200W

- サーバブレード消費電力仕様：定格電力(最大消費電力)400W,
  最もパワーキャッピングをかけたときの最大消費電力 150W
- サーバブレード搭載数：4 台
- サーバブレード 0，1 の運用時電力制御(APC)を無効に設定

  → システム装置の消費電力合計が，運用時電力制御上限値超過時は，サーバブレード 2，3 でキャッピングがかかり，1200W から電力制御を無効に設定したサーバブレード 0，1 の定格 400W×2 を引いた 400W をサーバブレード 2，3 で分け合うため，200W/サーバブレードに電力制限されます。

重要 次の例のように，サーバブレードで使用可能な消費電力から，電力制御を無効に設定したサーバブレードの定格を引いた値を残りのサーバブレードで分け合う際に，残りのサーバブレードの最もパワーキャッピングをかけたときの最大消費電力を下回るケースでは，電力制御の無効設定はできません。

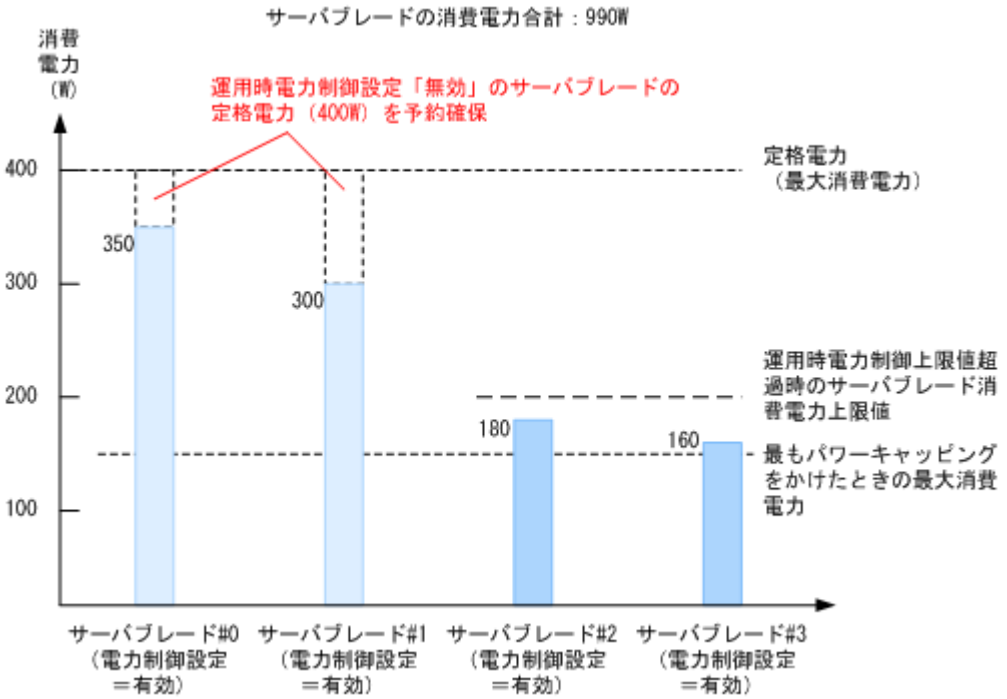
- システム装置の運用時電力制御上限値：2000W
- サーバブレード以外の消費電力：700W

  → サーバブレードで使用可能な消費電力：1300W
- サーバブレード消費電力仕様：定格電力(最大消費電力 400W,
  最もパワーキャッピングをかけたときの最大消費電力：150W
- サーバブレード搭載数：4 台
- サーバブレード 0，1，2 を電力制御無効に設定

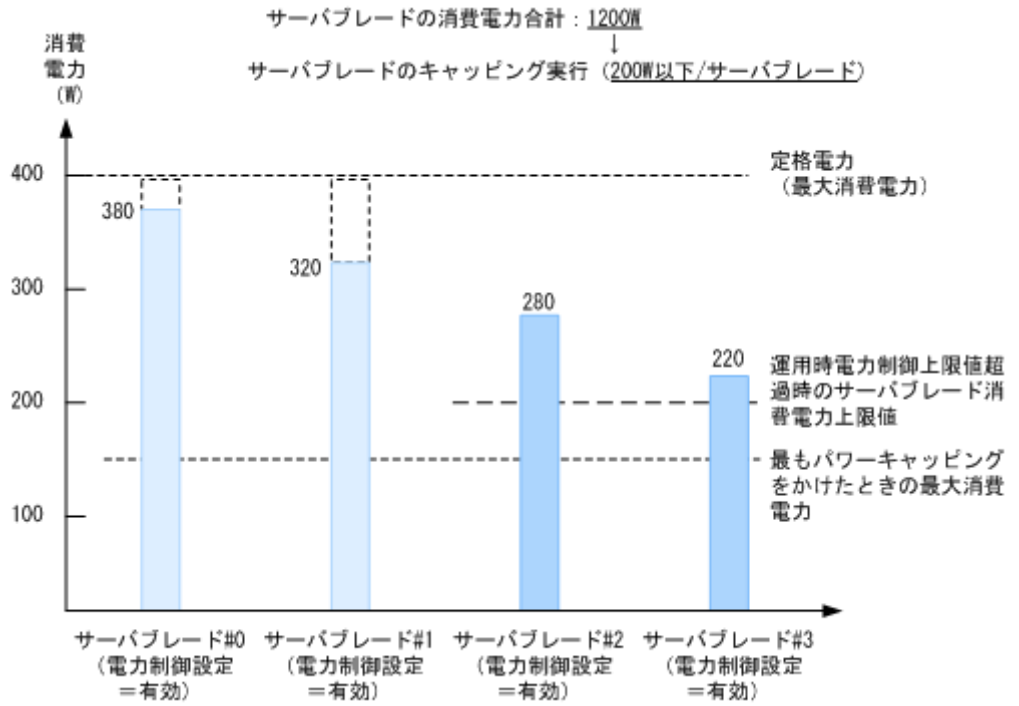
  → システム装置の消費電力合計が，運用時電力制御上限値超過時は，サーバブレード 3 でキャッピングがかかるが，1300W から，電力制御を無効に設定したサーバブレード 0，1，2 の定格 400W×3 を引いた 100W は，最もパワーキャッピングをかけたときの最大消費電力 150W を下回るため，この電力制御の無効設定はできない。

---

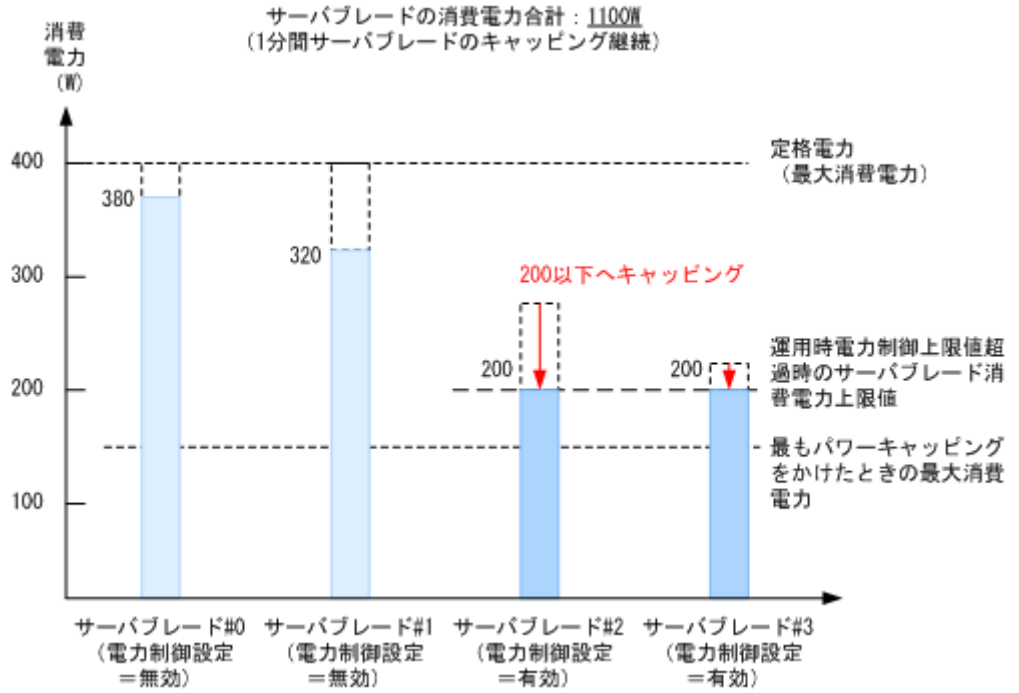
1. 通常運転状態



2. システム装置の消費電力合計が「運用時電力制御上限値」を超過



3. サーバブレードのキャッピングにより，システム装置の消費電力合計を「運用時電力制御上限値」以下へ制御



4. 1 分経過後にキャッピング解除

   →手順 1 に戻る。

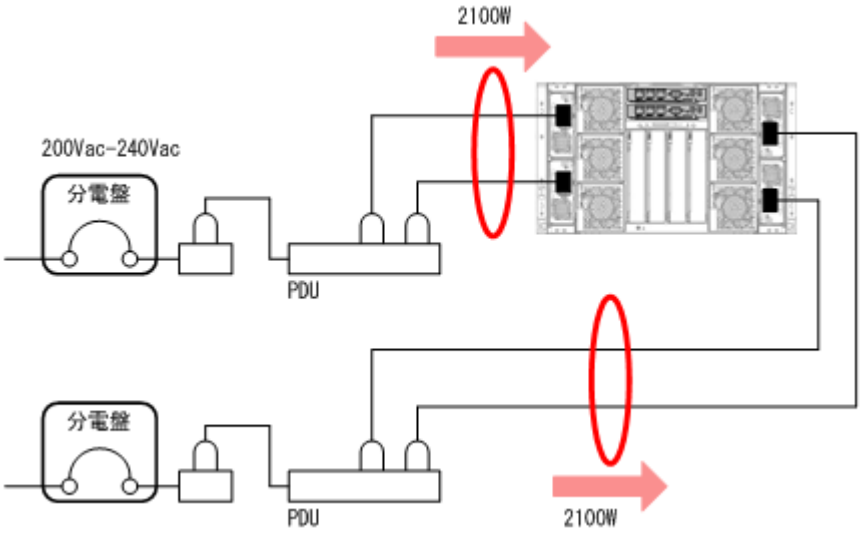
2.20.5 電源容量拡張機能

電源冗長構成において, 待機系の余剰電力を利用することで電源冗長正常時(主系/待機系ともに正常時)に電力設備の最大供給電力まで使用可能電力を拡張する機能を提供します。本機能により，サーバブレードの搭載制限やサーバブレードのパワーキャッピングによる性能制限を緩和することが可能です。

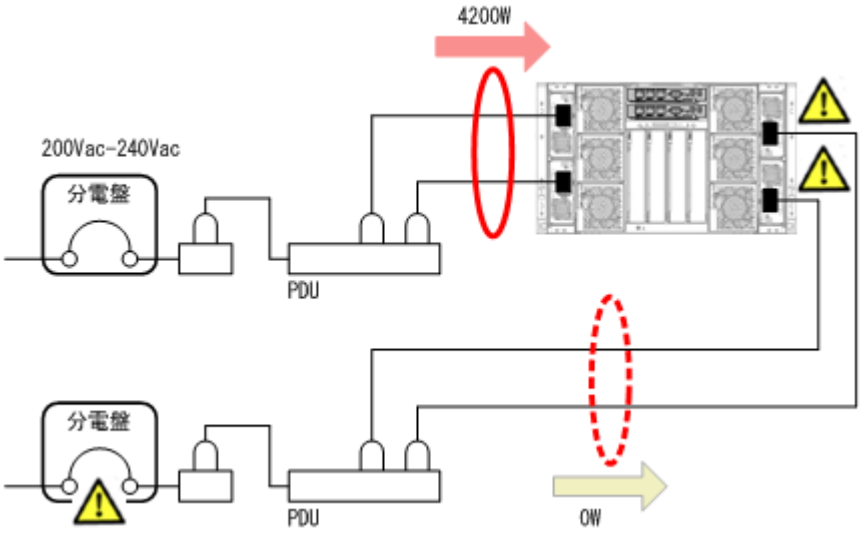
電源冗長異常時には，一時的に電力設備の最大供給電力で動作させた後で，高速なサーバブレードのパワーキャッピングにより，使用可能電力を定格内に戻すことで，システム装置内蔵の電源モジュールの電力許容量を超える電力過負荷状態から保護します。本機能実現のため，一時受電能力を向上させた電源モジュールを採用しています。

(1) 電源容量拡張機能＝無効時の動作概要

- 冗長電源正常時:最大供給電力 4200W
  2 つの電源系統からそれぞれ 2100W ずつ供給されます。

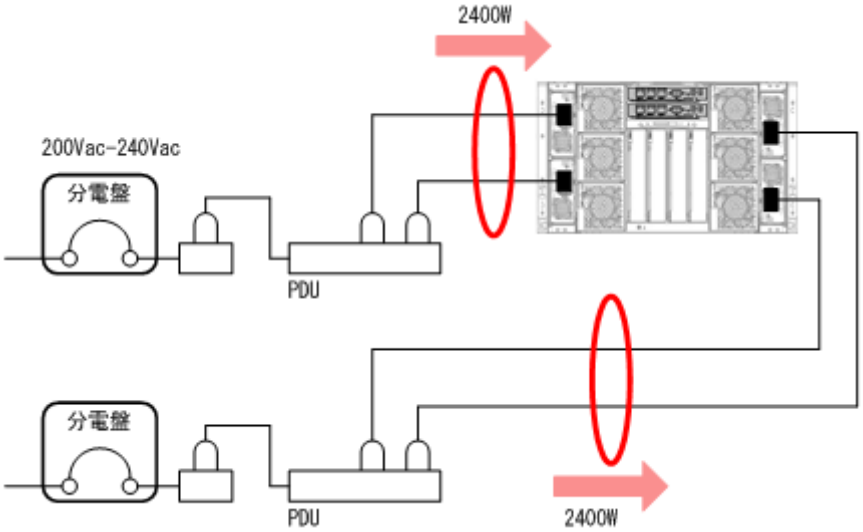


- 冗長電源異常時:最大供給電力 4200W
  1 つの電源系統で障害が発生すると，もう一方の電源系統から 4200W 供給されます。

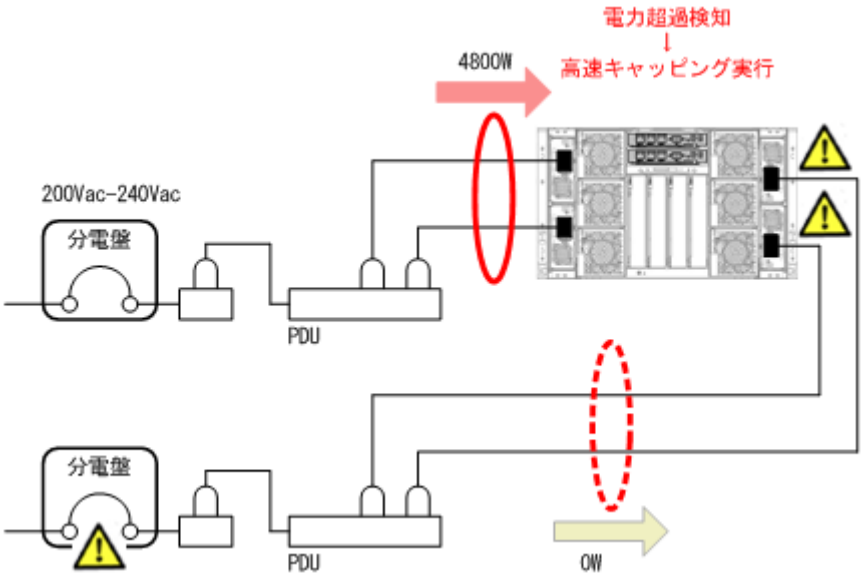


(2) 電源容量拡張機能＝有効(デフォルト)時の動作概要

- 冗長電源正常時:最大供給電力 4800W(600W 電源容量拡張)
  2 つの電源系統からそれぞれ 2400W ずつ供給されます。



- 冗長電源異常発生時:最大供給電力 4800W(電源容量拡張分を高速キャッピング)
  １つの電源系統で障害が発生すると，もう一方の電源系統から 4800W 供給されます。電源モジュールの定格受電能力を超えているため，電源容量拡張分を高速キャッピングします。



- 冗長電源異常時:最大供給電力 4200W(電源容量拡張機能＝無効時と同等)
  正常な電源系統には 4200W(電源容量拡張機能＝無効時と同等)が供給されます。

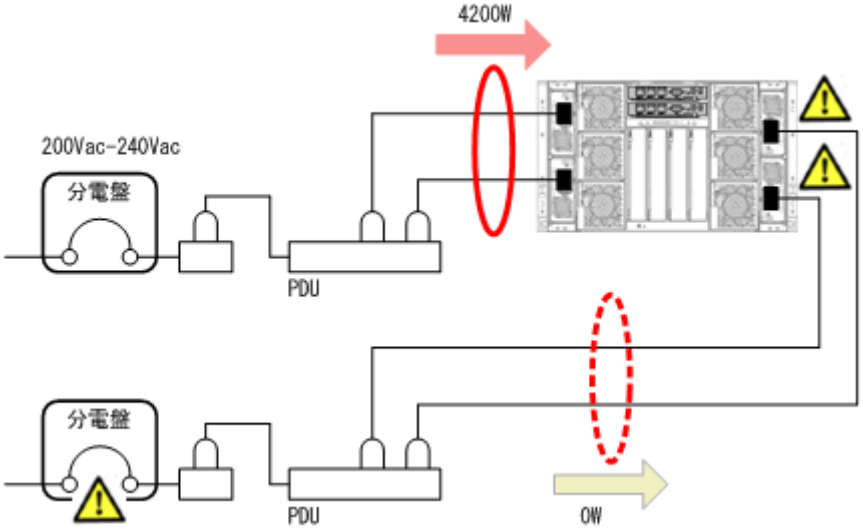


表 2-109 Web コンソールでの操作方法

項目	画面
電源容量拡張機能の表示，設定	Resources タブ → Systems → 電力管理

2.20.6 電力値のモニタリング表示

マネジメントモジュールのコンソールでは，システム装置全体やサーバブレードなどの電力値に関する情報を確認することができます。

消費電力情報は，現在値表示と履歴表示の 2 つがあり，履歴表示では前日の 24 時間分のデータを確認することができます。

SMP 構成の場合，プライマリサーバブレードの消費電力情報が，SMP を構成するすべてのサーバブレードの消費電力の合計値を示します。

CPU 周波数はサーバブレード単位に表示します。サーバブレード内の複数の CPU の周波数は同一の値をとります。

表 2-110 Web コンソールでの操作方法

項目	画面
電力値の現在値表示	Resources タブ → Systems → 電力管理
電力値の履歴表示	Resources タブ → Systems → 電力管理 → Action → シャーシ電力履歴のダウンロード

表 2-111 CLI コンソールでの操作方法

項目	コマンド
電力値の履歴表示	show log power

2.20.7 電源容量超過時のサーバブレード強制電源 OFF 順序設定

電源モジュールの故障などで，現在使用している消費電力分の電力供給が行えなくなった場合，マネジメントモジュールはサーバブレードの電源を強制的に OFF し，稼働しているサーバブレードを電力供給が行える分のみに制限します。この際，マネジメントモジュールがどのサーバブレードから順に電源 OFF するかを設定することが可能です。

システム装置出荷時は，サーバブレード 7 → 6 → 5 → 4 → 3 → 2 → 1 → 0 の順で電源 OFF する設定となっています。

表 2-112 Web コンソールでの操作方法

項目	画面
電源容量超過時のサーバブレード強制電源 OFF 順序設定の表示，設定	Resources タブ → Systems → 電力管理

2.20.8 電源モジュール最適制御機能

電源モジュール最適制御機能は，稼働させるサーバブレード数に応じて，アクティブにする電源モジュール数を静的に最適化することで，電源モジュールを高効率負荷帯域で動作させる機能です。

「有効」がデフォルト設定されています。

本機能を「有効」とすることで，停止している電源モジュールの電源 LED が緑に点滅します。

表 2-113 Web コンソールでの操作方法

項目	画面
電源モジュール最適制御機能設定の表示	Resources タブ → Systems → 電力管理
電源モジュール最適制御機能設定の設定	Resources タブ → Systems → 電力管理 → 電源モジュール最適制御機能設定(アクションメニュー)

表 2-114 CLI コンソールでの操作方法

項目	コマンド
電力設定の表示	show power ps-module
電力設定の変更	set power ps-module

2.21 DCMI 機能

DCMI 機能について説明します。

2.21.1 DCMI 概要

BS500 は，DCMI(Data Center Manageability Interface) version 1.5 に対応しています。サーバブレード上の OS や LAN で接続された外部の管理 PC から DCMI コマンド(IPMI command ベース)を DCMI 対応サーバブレードの BMC へ発行することにより，電源管理や各種環境値のモニタリング等を行うことができます。

DCMI を利用する場合，事前にサーバシャーシの DCMI モードを"有効"に設定する必要があります。DCMI モード有効の場合にのみ，DCMI 対応のサーバブレードは DCMI コマンドを受け付けることが可能になります。DCMI モード有効の場合でも DCMI 非対応のサーバブレードは DCMI コマンドを受け付けることができません。

重要

- DCMI と APC(Accurate Power Control)を同時に有効にすることはできません。DCMI モードを有効にした場合，APC は自動的に無効となり APC に関する設定変更は行えません。
- DCMI モードの有効/無効の切り替えは，以下の場合に行えます。
  - サーバシャーシ内のすべてのブレードの初期化が終了していること
  - サーバシャーシ内の DCMI 対応ブレードのメイン電源が OFF であること
- DCMI モードを有効に設定した場合，APC の設定内容は初期化されます。同様に DCMI モードを無効に設定した場合も，DCMI の設定内容は初期化されます。
- DCMI と EPC(Emergency Power Control)は同時に利用することができます。電源障害などにより供給電力が不足する状況となった場合，装置の継続稼働のため EPC によるパワーキャッピングが優先して実行されます。

2.21.2 DCMI に対応するサーバブレード

DCMI を使用するには，サーバブレードが DCMI に対応している必要があります。対応するサーバブレードについては「*BladeSymphony BS500 システム概要*」を参照してください。

2.21.3 DCMI モードの設定方法

1. DCMI モードの切り替え

   DCMI モードを設定するには，Web コンソールまたは CLI コンソールを使用します。

DCMI モードが切り替わる設定変更を行うと，DCMI 対応サーバブレードが自動的に再初期化されます。

表 2-115 Web コンソールでの操作方法

項目	画面
DCMI モードの切り替え	Resources タブ → Systems → 電力管理→Action→DCMI モード設定

表 2-116 CLI コンソールでの操作方法

項目	画面
DCMI モードの切り替え	set power dcmi-mode

2. ブレードの初期化終了の確認

   DCMI モードを変更して DCMI 対応サーバブレードの再初期化が実行された場合，システムイベン トログを確認し，対象サーバブレードの初期化が終了したことを確認してください。

   Web コンソールから確認する場合，［Resources］タブー［Modules］のツリービューから［サーバブレード］ー目的のサーバブレードを選択し，サーバブレードの［状態］タブー［初期化状態］が［正常終了］となっていることを確認してください。

重要

- DCMI 対応サーバブレードの統合ファームウェア更新中に DCMI モードの切り替えを行わないでください。
- DCMI モードの切り替えは，全ての DCMI 対応サーバブレードが統合ファームウェアの更新中でないことを確認したうえで行ってください。
- 統合ファームウェアの更新を行った場合，システムイベントログを確認し対象サーバブレードの初期化が終了したことを確認してください。
- Web コンソールから確認する場合，［Resources］タブー［Modules］のツリービューから［サーバブレード］ー目的のサーバブレードを選択し，サーバブレードの［状態］タブー［初期化状態］が ［正常終了］となっていることを確認してください。
- DCMI 対応マネジメントモジュールファームウェアから非対応のファームウェアにダウングレードする場合， 事前に DCMI モードを「無効」に設定してください。DCMI モード有効のままダウングレードすると， APC 機能が正常に動作しない場合があります。

2.21.4 対応 DCMI コマンド一覧

DCMI version 1.5 で定義されるコマンドのうち，BS500 でサポートしているものについては下記表を参照してください。

表 2-117 対応 DCMI コマンド一覧

DCMI command	NetFn	CMD	Min Privilege level	BS500 でのサポート
Get DCMI Capabilities Info	DCGRP (2Ch, 2Dh)	01h	Session-less	○
Set DCMI Configuration Parameters	DCGRP (2Ch, 2Dh)	12h	Admin	○
Get DCMI Configuration Parameters	DCGRP (2Ch, 2Dh)	13h	User	○
Get Management Controller Identifier String	DCGRP (2Ch, 2Dh)	09h	User	○
Set Management Controller Identifier String	DCGRP (2Ch, 2Dh)	0Ah	Admin	○
Get Asset Tag	DCGRP (2Ch, 2Dh)	06h	User	○
Set Asset Tag	DCGRP (2Ch, 2Dh)	08h	Operator	○

DCMI command	NetFn	CMD	Min Privilege level	BS500 でのサポート
Get Device ID	App (06h)	01h	User	○
Get System GUID	App (06h)	37h	User	○
Get Chassis Capabilities	Chassis (00h)	00h	User	○
Get Chassis Status	Chassis (00h)	01h	User	○
Chassis Control	Chassis (00h)	02h	Operator	○
Chassis Identify	Chassis (00h)	04h	Operator	○
Get ACPI Power State	App (06h)	07h	User	○
Set System Boot Options	Chassis (00h)	08h	Operator	× ※
Get System Boot Options	Chassis (00h)	09h	Operator	○
Get SEL Info	Storage (0Ah)	40h	User	○
Reserve SEL	Storage (0Ah)	42h	User	○
Get SEL Entry	Storage (0Ah)	43h	User	○
Clear SEL	Storage (0Ah)	47h	Operator	○
Get DCMI Sensor Info	DCGRP (2Ch, 2Dh)	07h	Operator	○
Get SDR Repository Info	Storage (0Ah)	20h	Operator	○
Reserve SDR Repository	Storage (0Ah)	22h	Operator	○
Get SDR	Storage (0Ah)	23h	User	○
Get Sensor Threshold	S/E (04h)	27h	Operator	○
Get Sensor Reading	S/E (04h)	2Dh	User	○
Set Sensor Event Enable	S/E (04h)	28h	Operator	×
Get Sensor Event Enable	S/E (04h)	29h	User	×
Get Power Reading	DCGRP (2Ch, 2Dh)	02h	User	○
Get Power Limit	DCGRP (2Ch, 2Dh)	03h	User	○
Set Power Limit	DCGRP (2Ch, 2Dh)	04h	Operator	○
Activate/Deactivate Power Limit	DCGRP (2Ch, 2Dh)	05h	Operator	○
Set Thermal Limit	DCGRP (2Ch, 2Dh)	0Bh	Operator	○
Get Thermal Limit	DCGRP (2Ch, 2Dh)	0Ch	User	○
Get Temperature Readings	DCGRP (2Ch, 2Dh)	10h	User	○
Reset Watchdog Timer	App (06h)	22h	Operator	○
Set Watchdog Timer	App (06h)	24h	Operator	○
Get Channel Authentication Capabilities	App (06h)	38h	None	○
Set Session Privilege Level	App (06h)	3Bh	User	○
Close Session	App (06h)	3Ch	User	○
Get Session Info	App (06h)	3Dh	User	○
Get Payload Activation Status	App (06h)	4Ah	User	○
Get Payload Instance Info	App (06h)	4Bh	User	○
Get Channel Payload Support	App (06h)	4Eh	User	○
Activate Payload	App (06h)	48h	Configurable	○
Deactivate Payload	App (06h)	49h	Configurable	○
Get Channel Cipher Suites	App (06h)	54h	None	○
SOL Activating	Transport (20h)	20h	None	○

DCMI command	NetFn	CMD	Min Privilege level	BS500 でのサポート
Set LAN Configuration Parameters	Transport (0Ch)	01h	Admin	○
Get LAN Configuration Parameters	Transport (0Ch)	02h	Operator	○
Set Channel Access	App (06h)	40h	Admin	○
Get Channel Access	App (06h)	41h	User	○
Get Channel Info	App (06h)	42h	User	○
Set User Access	App (06h)	43h	Admin	○
Get User Access	App (06h)	44h	Operator	○
Set User Name	App (06h)	45h	Admin	○
Get User Name	App (06h)	46h	Operator	○
Set User Password	App (06h)	47h	Admin	○
Set User Payload Access	App (06h)	4Ch	Admin	○
Get User Payload Access	App (06h)	4Dh	Operator	○
Set SOL Configuration Parameters	Transport (0Ch)	21h	Admin	○
Get SOL Configuration Parameters	Transport (0Ch)	22h	User	○
Set BMC Global Enables	App (06h)	2Eh	system interface	○
Get BMC Global Enables	App (06h)	2Fh	system interface, User	○
Clear Message Flags	App (06h)	30h	system interface	○
Get Message Flags	App (06h)	31h	system interface	○
Get Message	App (06h)	33h	System Interface	○
Send Message	App (06h)	34h	User	○

※コマンドは正常に終了しますが，設定は反映されません。

2.22 静音モード機能

システム装置の静音モード機能について説明します。

2.22.1 静音モード機能概要

静音モードは，FAN 回転数を抑えることで騒音・消費電力の低減を優先させる動作モードです。入気温度 30℃以下において最も静音効果が発揮されます。

表 2-118 Web コンソールでの操作方法

項目	画面
静音モードの表示，設定	Resources タブ → Modules → シャーシ → Action → 静音モード設定

重要

- ロングライフサポートサービス専用シャーシでは本機能は使用できません。
- 本機能で使用できるサーバブレード，およびスイッチモジュール種別，搭載できるモジュール数には制限があります。

  - サポート対象のサーバブレード

E5-2430L CPU を搭載するサーバブレード(BS520A サーバブレード A1 モデル)

- サポート対象のスイッチモジュール

Brocade 10 Gb DCB スイッチモジュール，10Gb LAN パススルーモジュール，Brocade 8/16Gb ファイバチャネルスイッチモジュールおよび Brocade 16Gb ファイバチャネルスイッチモジュールを除くスイッチモジュール

- 搭載できるモジュール数

電源モジュール 1 台あたりの出力が約 560W(AC100V 入力時)，約 760W(AC200V 入力時)を超過した場合，静音効果は低下する場合があります。

- 本機能を有効設定する際は，次の操作が必要となります。

  - 電源モジュール最適制御機能の無効設定

  - サポート対象外サーバブレードのメイン電源オフ

- 本機能を有効設定した場合，サポート対象外サーバブレードのメイン電源オンは抑止されますのでご注意ください。

  一方，サポート対象外スイッチモジュールが搭載されている場合，サーバブレードのメイン電源オンは抑止されませんが，静音効果は低下する場合があります。

- 騒音値を基準とし，CPU の動作周波数を制御します。そのため，本機能を有効設定した場合，高温環境では通常時と比べて CPU 性能が低下する場合があります。

- 電源モジュール，およびファンモジュール故障時には，静音効果は低下する場合があります。

- 静音モードの無効設定は即時適用されますが，有効設定には約 1 分程度時間を要します。

2.23 SNMP 機能

マネジメントモジュールの SNMP 機能について説明します。

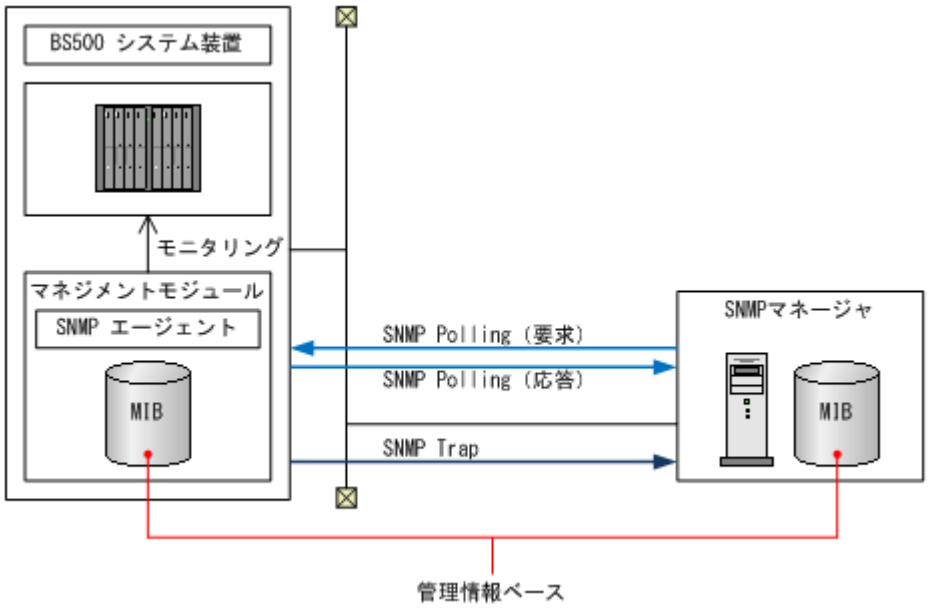
2.23.1 SNMP 機能概要

SNMP 機能により実現できる機能は次のとおりです。

表 2-119 SNMP 機能

項目	内容
ポーリング機能	システム装置を SNMP マネージャから監視対象として認識することが可能となります。また，システム装置が独自に定義した管理情報ベース（MIB）の各種取得項目に対して，情報取得要求を実施した場合，MIB に定義した情報に対応する応答が返答されます。 ポーリング機能は，マネジメントモジュールに登録した SNMP マネージャの IP アドレスからの要求に対してのみ，応答します。
トラップ機能	システム装置が独自に定義した管理情報ベース（MIB）にしたがって，マネージャに対して自発的に情報通知を行います。このため，SNMP マネージャによる障害監視が可能になります。※

※SNMP 標準トラップはサポート対象外です。



SNMP ポーリング機能の諸元は次のとおりです。

表 2-120 SNMP ポーリング機能の諸元

項目	内容
サポート命令	SNMPv1/v2c/v3（Get，GetNext，GetBulk）
最大同時通知 SNMP マネージャ数	8
サポートモジュール種別	サーバブレード，マネジメントモジュール，スイッチモジュール，電源モジュール，ファンモジュール

SNMP トラップ機能の諸元は次のとおりです。

表 2-121 SNMP トラップ機能の諸元

項目		内容
通知手段		SNMP（SNMPv2Trap/SNMPv3Trap）
最大同時通知 SNMP マネージャ数		8
通知契機		マネジメントモジュールの障害 SEL 契機
通知内容	第 1 変数バインディング※1※2	アラートの送信時刻
	第 2 変数バインディング※1※2	アラートが発生したシャーシの ID
	第 3 変数バインディング※1※2	アラートのレベル
	第 4 変数バインディング※1※2	アラートの ID
	第 5 変数バインディング※1※2	アラートのメッセージ
	第 6 変数バインディング※1	アラートが発生した部位
	第 7 変数バインディング※2	アラートが発生したモジュールの種別
	第 8 変数バインディング※2	アラートが発生したモジュールの位置
	第 9 変数バインディング※2	アラートが発生したモジュールの名称
	第 10 変数バインディング※2	アラートが発生したモジュールの製造番号
	第 11 変数バインディング※2	アラートのイベントコード

※1：SNMP トラップフォーマットを BSM に設定した場合

※2：SNMP トラップフォーマットを HCSM に設定した場合

SNMPv3 機能の諸元は次のとおりです。

表 2-122 SNMPv3 機能の諸元

項目	内容
認証方式(ハッシュ方式)	MD5/SHA-1
暗号化方式	DES/AES128

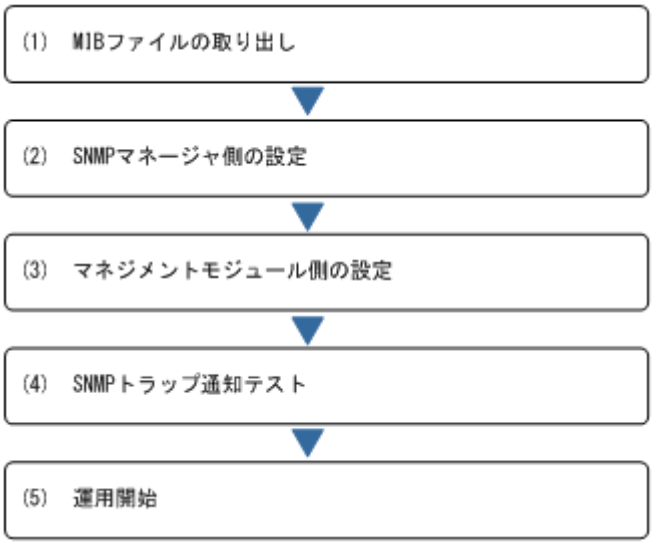
2.23.2 前提条件

SNMP 機能を使用する際の前提条件を次に記します。

- SNMP トラップを受信する SNMP マネージャは，SNMPv1/v2c/v3 に対応していること。
- マネジメントモジュールと SNMP マネージャが動作する管理サーバ間が，ネットワークで通信できる環境にあること。

2.23.3 SNMP 機能の設定手順

マネジメントモジュールで SNMP 機能を利用する際の設定手順は次のとおりです。



(1) MIB ファイルの取り出し

本システム装置を管理するための MIB ファイルは，マネジメントモジュールのコンソールから取り出すことができます。

マネジメントモジュールのファームウェアバージョンが更新され，新しい OID が追加された場合は，マネジメントモジュールのファームウェアバージョンの更新後に，再度取り出してください。マネジメントモジュールから取り出せる MIB のバージョンも，マネジメントモジュールのコンソールから確認することができます。

表 2-123 Web コンソールでの操作方法

項目	画面
MIB ファイルの取り出し	Administration タブ → SNMP → MIB タブ → MIB ファイルダウンロード
MIB ファイルのバージョン表示	Administration タブ → SNMP → MIB タブ

表 2-124 CLI コンソールでの操作方法

項目	コマンド
MIB ファイルの取り出し	export snmp mib
MIB ファイルのバージョン表示	show snmp mib

(2) SNMP マネージャ側の設定

ご使用される SNMP マネージャに対して，次の操作を実施してください。操作手順は SNMP マネージャのマニュアルを参照してください。

- MIB ファイルの登録
- トラップイベントの登録
- ポーリング機能で取得する MIB 項目の選択と，値を取得するために必要な設定

トラップイベントの内容，取得できる MIB 項目の内容は，「*BladeSymphony BS500 MIB ユーザーズガイド*」を参照してください。

(3) マネジメントモジュール側の設定

マネジメントモジュールのコンソールから次の設定を実施してください。設定は，大きくエージェント設定とマネージャ設定に分かれ，エージェント設定にはマネジメントモジュール自身の情報，マネージャ設定には接続する SNMP マネージャの情報を設定します。

各設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

エージェント設定

エージェントの設定項目は次の 7 項目です。

- SNMP 機能の有効/無効
- System Contact Name
- System Location
- ポート番号
- トラップレベル
- SNMP バージョン
- エンジン ID 作成文字列

マネージャ設定

マネージャの設定項目は次の 10 項目です。

- IP アドレス/ホスト名
- ポート番号
- SNMP バージョン
- Community Name
- User Name
- アクセス種別
- 認証種別
- 認証パスワード

- 暗号化種別
- 暗号化パスワード

表 2-125 Web コンソールでの操作方法

項目	画面
SNMP エージェント設定の表示，設定	Administration タブ → SNMP → SNMP エージェントタブ
SNMP マネージャ設定の表示，設定	Administration タブ → SNMP → SNMP マネージャタブ

表 2-126 CLI コンソールでの操作方法

項目	コマンド
SNMP エージェント設定の表示	show snmp agent
SNMP エージェント設定の設定	set snmp agent
SNMP マネージャ設定の表示	show snmp manager
SNMP マネージャ設定の設定	set snmp manager

重要 SNMP バージョン v1/v2c を利用する IPv6 アドレスの SNMP マネージャを登録する場合，SNMP マネージャのホスト名には IPv6 アドレスを指定してください。ホスト名を指定した場合，SNMP マネージャ上で当該マネジメントモジュールがノードとして検出されません。
SNMP バージョン v1/v2c を利用する IPv4 アドレスの SNMP マネージャを登録する場合は，IPv4 アドレス，ホスト名を指定することができます。
SNMP バージョン v3 を利用する SNMP マネージャを登録する場合は，SNMP マネージャのアドレスが IPv4，IPv6 にかかわらず，ホスト名として，IP アドレス，ホスト名どちらも指定することができます。

参考 マネジメントモジュールのセキュリティ強度設定を"高"に設定した場合，SNMP の設定を以下としてください。

- エージェント設定
  - SNMP バージョン：v1/v2/v3
- マネージャ設定
  - SNMP バージョン：v3
  - アクセス種別：AuthPriv
  - 認証種別：SHA
  - 暗号化種別：AES

設定していない場合，マネージャからの要求に対して無応答となり，SNMP トラップを発行しません。

(4) SNMP トラップ通知テスト

マネジメントモジュールのコンソールから SNMP トラップ通知のテストを実行し，正しく SNMP マネージャにトラップが通知されるか確認してください。トラップが通知されない場合，ネットワークの環境，SNMP マネージャ，およびマネジメントモジュールの設定を見直してください。

表 2-127 Web コンソールでの操作方法

項目	画面
SNMP トラップ通知テスト	Administration タブ → SNMP → SNMP トラップ送信（アクションメニュー）

表 2-128 CLI コンソールでの操作方法

項目	コマンド
SNMP トラップ通知テスト	test snmp trap

(5) 運用開始

設定された項目に従い，SNMP 機能を運用します。システム装置の障害を検出した際は，必要に応じてダンプログを採取してください。ダンプログの詳細は「2.28 ログ」を参照してください。

2.23.4 SNMP トラップメッセージの選択

SNMP トラップで通知するメッセージは，JP1/ServerConductor/Blade Server Manager に通知するアラートメッセージに基づくメッセージと，HCSM に通知するアラートメッセージに基づくメッセージの 2 種類から選択することができます。この 2 種類はメッセージの分類の仕方が異なるだけであり，どちらを選択いただいても通知されるトラップメッセージの情報量は同等です。また，JP1/ServerConductor/Blade Server Manager や HCSM を併用されている場合に，本選択の設定を使用されているミドルウェアに合わせる必要はありません。

従来機種の BladeSymphony で JP1/ServerConductor/Blade Server Manager に通知するアラートに基づくメッセージのみをサポートしている装置と一緒に本装置を管理する場合は，JP1/ServerConductor/Blade Server Manager に通知するアラートに基づくメッセージを選択することを推奨します。

参考 JP1/ServerConductor/Blade Server Manager に通知するアラートに基づくメッセージと HCSM に通知するアラートに基づくメッセージで，SNMP トラップイベント名と OID の値は異なります。詳細は「*BladeSymphony BS500 MIB ユーザーズガイド*」を参照してください。

表 2-129 Web コンソールでの操作方法

項目	画面
SNMP トラップメッセージ選択設定の表示，設定	Administration タブ → SNMP → トラップメッセージ タブ

表 2-130 CLI コンソールでの操作方法

項目	コマンド
SNMP トラップメッセージ選択設定の表示	show snmp trap-message
SNMP トラップメッセージ選択設定の設定	set snmp trap-message

2.24 E-mail 通報機能

マネジメントモジュールの E-mail 通報機能について説明します。

2.24.1 E-mail 機能概要

E-mail 機能として，次に示す通報手段があります。

(1) 障害契機通報

システム装置に障害が発生した時，障害解析に必要なログ情報を採取し，E-mail に添付し通報します。障害契機通報の履歴をマネジメントモジュール内に保存します。履歴は最大 32 通報分保存し，保存個数を超過した場合は古い履歴から削除します。

(2) ログ出力契機通報

サーバブレードでログが出力されたとき，ログを E-mail に添付し通報します。本メールは障害契機通報の補足的な情報を通知するものです。

(3) 手動契機通報（現状通報）

現在のシステム装置の状態についての情報を採取し，E-mail に添付し通報します。

(4) 手動契機通報（履歴選択通報）

障害契機通報の履歴から任意の履歴を選択して再度送付することができます。例えばシステム装置に障害が発生した時，メールサーバが停止中で障害契機通報に失敗した場合，メールサーバ回復後に改めて通報することができます。

参考 人手によるサーバブレードのログ出力によっても，「(2) ログ出力契機通報」が実施されます。この場合は，本メールの前後に障害契機通報によるメールが存在しません。

2.24.2 前提条件

E-mail 通報機能を使用する際の前提条件を次に示します。

- E-mail 通報機能は，マネジメントモジュールがメールクライアントとなって，メールサーバ（SMTP サーバ）に E-mail を送信する機能です。このため，別途 SMTP サーバが必要になります。
- マネジメントモジュールが，メールサーバと通信できる環境にあることが必要です。

2.24.3 E-mail 通報機能諸元

E-mail 通報機能の諸元を次に示します。

表 2-131 E-mail 通報機能の諸元

項目			内容
通報手段			E-mail(SMTP 準拠)
登録可能宛先個数			4
登録可能 SMTP サーバ個数			1
通報契機			• 障害発生時 • サーバブレードのログ出力時 • 手動での通報(現状通報，障害履歴通報)
通報リトライ			障害契機通報またはログ出力契機通報が失敗した場合，通報のリトライを実施します。
通報内容	障害契機通報	件名	[AUTO] Failure report.
		本文	メール説明：「下記装置で障害が発生しました。」 サーバシャーシ情報 障害情報（概要）
		添付 ※1	svpsts-YYYYMMDD-hhmmss.gz trc-YYYYMMDD-hhmmss.tar.gz※2 marlog.gz
	ログ出力契機通報	件名	[AUTO] Log dump report.
		本文	メール説明：「下記装置でサーバブレードのログが出力されました。」
		添付 ※1	次のいずれかのファイル hvmdumpN-YYYYMMDD-hhmmss.gz raslogN-YYYYMMDD-hhmmss.tar.gz
	手動契機通報(現状通報)	件名	[MANUAL] Current status report.
		本文	メール説明：「本メールは，人手操作で送付されたものです。装置の現在の状態を示すログを送付します。」

項目			内容
			サーバシャーシ情報
		添付※1	svpsts-YYYYMMDD-hhmmss.gz trc-YYYYMMDD-hhmmss.tar.gz※2
	手動契機通報(障害履歴通報)	件名	[MANUAL] History report.
		本文	障害契機通報時と同じ内容
		添付※1	障害契機通報時と同じ内容
SMTP 認証方式			認証なし／ PLAIN ／ LOGIN ／ CRAM-MD5 より選択可能
暗号化			暗号化なし ／ SSL ／ TLS より選択可能

※1：添付ファイル名の凡例で YYYYMMDD-hhmmss は通報開始時刻を示します。(YYYY：西暦，MM：月，DD：日，hh：時，mm：分，ss：秒，N：サーバブレード番号（0～7）を示します)

※2：E-mail アドレス設定で，「ログ添付」が無効となっている宛先には添付されません。

通報時に添付する添付ファイルの諸元を次に示します。

表 2-132 添付ファイルの諸元

ファイル名	内容	最大サイズ 上段：自動通報時 下段：手動通報時
svpsts-YYYYMMDD-hhmmss.gz	装置情報	500KBytes 500KBytes
trc-YYYYMMDD-hhmmss.tar.gz	マネジメントモジュールのログ	1000KBytes 1500KBytes
hvmdumpN-YYYYMMDD-hhmmss.gz	サーバブレードのログ(HVM 関連)	3000KBytes 添付なし
raslogN-YYYYMMDD-hhmmss.tar.gz	サーバブレードのログ(H/W 関連)	2000KBytes 添付なし
marlog.gz	障害情報（障害契機通報の本文に含む情報と同じ)	1KBytes 添付なし

2.24.4 E-mail 通報機能の設定手順

マネジメントモジュールで E-mail 通報機能を利用する場合, 通報情報と宛先情報の二つを設定する必要があります。通報情報はマネジメントモジュール自身の設定と通報先 SMTP サーバの設定で，宛先情報は通報する E-mail アドレスの設定となります。

各設定項目は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」または「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

(1) 通報情報

E-mail 通報情報として，次の設定を行ってください。

E-mail 送信設定

E-mail を送信するための設定は次の 6 項目です。

- E-mail 通報機能
- 通報元 E-mail アドレス

- ホスト名
- コメント
- SMTP サーバ
- ポート番号

SMTP サーバ認証設定

SMTP サーバの認証設定は次の 3 項目です。

- SMTP 認証
- アカウント
- 認証方式

E-mail 通報暗号化設定

E-mail 通報の暗号化設定は次の項目です。

- SMTP 経路暗号化

参考 マネジメントモジュールのセキュリティ強度設定を"高"に設定した場合，E-mail 通報情報の経路暗号化バージョンを"TLS"，かつ SMTP 認証方式を"CRAM-MD5"と設定してください。設定していない場合，E-mail を送信しません。

(2) 宛先情報

E-mail 通報の宛先情報として次の設定を行ってください。

宛先情報

宛先情報は次の 3 項目です。

- ニックネーム
- E-mail アドレス
- ログ添付

表 2-133 Web コンソールでの操作方法

項目	画面
E-mail 通報情報の表示，設定	Administration タブ → E-Mail 遠隔通報 → 通報設定タブ
E-mail 宛先情報の表示，設定	Administration タブ → E-Mail 遠隔通報 → 宛先設定タブ

表 2-134 CLI コンソールでの操作方法

項目	コマンド
E-mail 通報情報の表示	show e-mail mgmt-lan
E-mail 通報情報の設定	set e-mail mgmt-lan notification
E-mail 宛先情報の追加，設定	set e-mail mgmt-lan address
E-mail 宛先情報の削除	delete e-mail mgmt-lan address

2.24.5 手動契機通報(現状通報)

E-mail 通報に関する設定が完了したら，手動契機通報(現状通報)を実施して，通報のテストを実施してください。通報先の E-mail アドレスは, 設定したアドレス一覧から選択します。個別指定と一括指定が選択可能です。

表 2-135 Web コンソールでの操作方法

項目	画面
E-mail 手動契機通報(現状通報)	Administration タブ → E-Mail 遠隔通報 → 現状通報 (アクションメニュー)

表 2-136 CLI コンソールでの操作方法

項目	コマンド
E-mail 手動契機通報(現状通報)	send e-mail latest mgmt-lan

参考

- ログ収集には数分間かかります。
- E-mail 通報機能は，メールサーバに正しく送信できた時点で正常終了とします。
- 複数の宛先に一括して送信した場合は，一つでも通報に失敗すると，すべての宛先の結果が失敗となる場合があります。

参考 通報が失敗する時は，通報結果メッセージと次を参考に，環境と設定の見直しを行ってください。

- マネジメントモジュールとメールサーバが通信可能か確認してください。
  通信不可の場合
  - LAN ケーブルが正しく接続されていることを確認してください。
  - マネジメントモジュールのネットワーク設定を確認してください。
  - メールサーバをホスト名で指定する場合，マネジメントモジュールのネットワーク設定で DNS の指定を行ってください。
- SMTP サーバ上で SMTP サービスが稼働しているか確認してください。
  稼働していない場合
  - SMTP サービスを起動してください。
- E-mail 通報機能の基本情報および宛先情報設定は正しいか確認してください。

手動契機通報結果のメッセージ一覧を次に示します。

表 2-137 手動契機通報結果メッセージ一覧

コード	メッセージ 内容
E0410	<Address %> Sending e-mail notification was canceled. Address is not set.
	【意味】宛先設定に誤りがあります。または，指定した宛先に対応するユーザが存在しません。 【対処】e-mail 宛先設定を見直してください。
E0411	<Address %> Sending e-mail notification was canceled. A communication error occurred.
	【意味】SMTP サーバとの通信中にエラーが発生しました。 【対処】LAN 接続を確認してください。
E0412	<Address %> Sending e-mail notification was canceled. Connecting to SMTP server failed.
	【意味】SMTP サーバとの接続に失敗しました。 【対処】e-mail 通報設定（全般）を見直してください。／SMTP サーバの状態を確認してください。／LAN 接続を確認してください。
E0413	<Address %> Sending e-mail notification was canceled. Failed to resolve host.
	【意味】SMTP サーバのホスト名から IP アドレスを求められませんでした。

コード	メッセージ 内容
	【対処】e-mail 送信設定を見直してください。／ネットワーク設定(DNS)を見直してください。／LAN 接続を確認してください。
E0414	<Address %> Sending e-mail notification was canceled. Configuration is invalid.
	【意味】smtp サーバの ip アドレスのフォーマットに誤りがあります。 【対処】e-mail 送信設定を見直してください。
E0415	<Address %> Sending e-mail notification was canceled. SMTP server does not support requested authentication type.
	【意味】SMTP サーバが e-mail 通報設定で指定した SMTP 認証方式をサポートしていません。 【対処】e-mail 通報設定（認証方式）を見直してください。
E0416	<Address %> Sending e-mail notification was canceled. SMTP authentication failed.
	【意味】SMTP 認証用ユーザ／パスワードに誤りがあります。 【対処】e-mail 通報設定（認証ユーザ／パスワード）を見直してください。
E0417	<Address %> Sending e-mail notification was canceled. SMTP server does not support SSL/TLS.
	【意味】SMTP サーバが e-mail 通報設定で指定した暗号方式をサポートしていません。 【対処】e-mail 通報設定（暗号）を見直してください。
E0418	<Address %> Sending e-mail notification was canceled. Program failed.
	【意味】予期しないエラーが発生しました。 【対処】お買い求め先か，保守員に連絡してください。
E0419	<Address %> Sending e-mail notification was canceled. E-mail address is invalid.
	【意味】宛先設定に誤りがあります。または，指定した宛先に対応するユーザが存在しません。 【対処】e-mail 宛先設定を見直してください。

2.25 バナー機能

2.25.1 ログインバナー機能

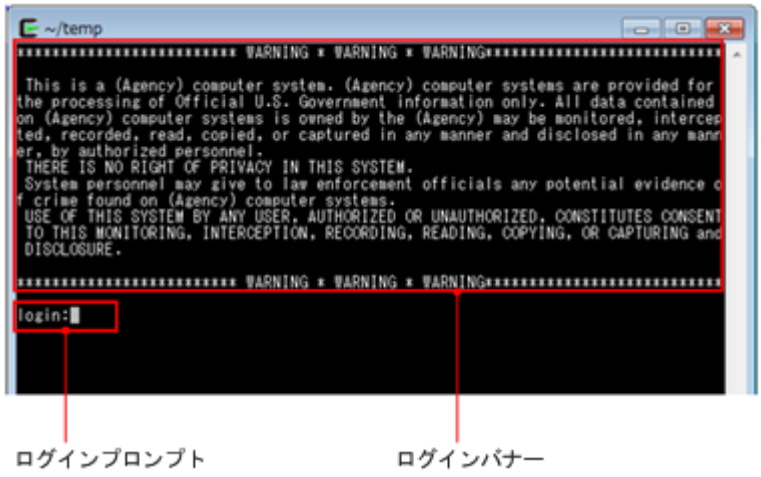
BS500 マネジメントモジュールにおけるログインバナー機能について説明します。

(1) ログインバナー機能の概要

ログインバナー機能は, マネジメントモジュールに接続したときにログインバナー(警告文)を表示する機能です。ログインバナーを表示する対象を下表に示します。

#	アクセス手段	バナー表示有無
1	CLI コンソール	表示する
2	web コンソール	表示する
3	LCD タッチパネル	表示しない

- CLI コンソールでの表示例：
  ログインプロンプト(login:)を表示する前に，設定されたバナー内容を表示します。



- web コンソールでの表示例：
  ログイン画面(User ID／Password 入力と同一の画面)に，設定されたバナー内容を表示します。

(2) ログインバナーの設定方法

ログインバナーとして設定できる内容は，下記です。

- メッセージ最大文字数：1599 文字(目安 80 文字*20 行)
- 入力可能文字種：英数字，記号，空白文字（ASCII 文字コード 0x20～0x7e），改行文字(LF)。ただし，"%"(ASCII 0x25)と"¥"(ASCII 0x5c)を除きます。日本語(半角カナ含む)やマルチバイト文字は使用できません。

表 2-138 Web コンソールでの操作方法

項目	画面
ログインバナーの設定	Administration タブ → ログインバナー → 編集

下記の項目を設定します。

- ログインバナー表示機能の有効／無効
- ログインバナーとして表示するテキスト内容を入力

参考

- 既にログインバナーが設定されている場合は，設定されているテキスト内容が表示されます。テキストを修正後，確認画面で［OK］ボタンを押すことで，ログインバナーが上書きされます。
- ログインバナー表示を無効に切り替えると，ログインバナーは表示しませんが，設定されているテキスト内容は保持しています。再度，ログインバナー表示を有効に切り替えると設定されていたテキスト内容を表示することができます。
- ログインバナーは，マネジメントモジュールの設定の保存でバックアップされます。したがって，設定の回復を実施すると，保存したときのログインバナーの状態になります。
- サーバブレードのリモートコンソールにおいてもログインバナー機能があります。リモートコンソールのログインバナーを有効にするためには，別途設定が必要です。詳しくは「*BladeSymphony BS500 リモートコンソールユーザーズガイド*」を参照ください。

2.26 USB ポートの無効化機能

USB デバイスの不正な使用を防ぐため，マネジメントモジュールの USB ポートを無効化することができます。USB ポート単位で設定を行うことができます。

表 2-139 Web コンソールでの操作方法

項目	画面
USB ポートの無効化/有効化の設定	Resources タブ → Modules → シャーシ → Action → フロントパネル USB 設定

表 2-140 CLI コンソールでの操作方法

項目	コマンド
USB ポートの無効化/有効化の設定	set chassis usb validity

2.27 インポート機能

マネジメントモジュールのインポート機能について説明します。

2.27.1 インポート機能の概要

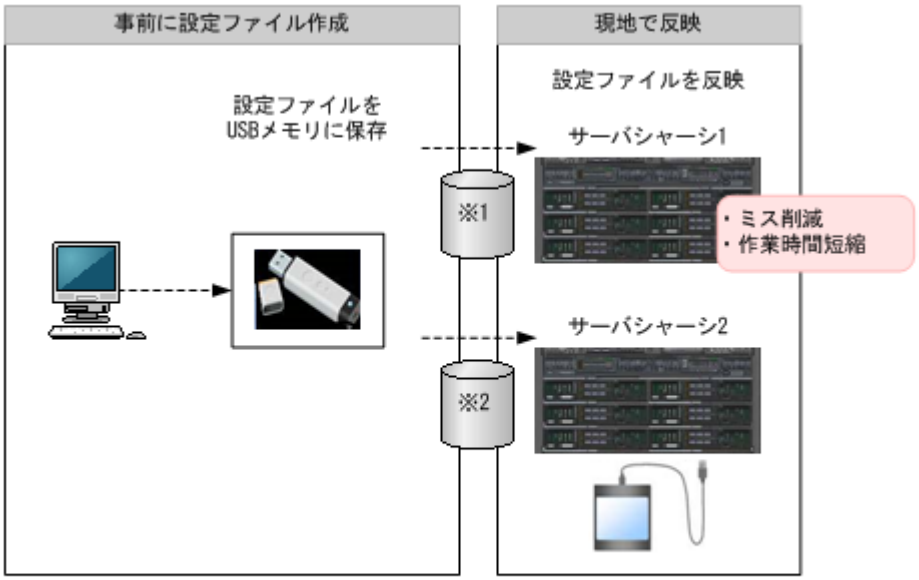
初期導入設定時に，サーバシャーシに一括設定を実施する機能です。

また，この時の設定ファイルをインポートファイルと呼びます。

インポートを実施する方法には，次の 2 種類があります。

- LCD タッチコンソールを使用
- Web コンソールを使用

図 2-8 LCD タッチコンソールを使用したときの例



注※1　サーバシャーシ1用設定ファイル
注※2　サーバシャーシ2用設定ファイル

(1)　インポート実施時の設定可能項目

インポートを実施することで設定可能な項目は次の 3 種類です。

- 時刻設定

  タイムゾーン設定と夏時間設定を行います。詳細は「2.2 時刻」を参照してください。
- プロトコル設定

  TELNET・SSH・FTP・HTTP・HTTPS の接続許可設定を行います。詳細は「2.4 セキュリティ」を参照してください。
- ネットワーク設定

  マネジメントモジュール・サーバブレード・スイッチモジュールの IP アドレス設定を行います。詳細は「2.3.6 IP アドレスの設定」を参照してください。

2.27.2 インポート実施方法

インポートの実施方法について説明します。

(1)　LCD タッチコンソールを使用する場合

LCD タッチコンソールを使用してインポートする手順を説明します。

準備するもの

- LCD タッチコンソール
- USB メモリ（バージョン：USB2.0）

参考 LCD タッチコンソール機能を無効に設定している場合および USB ポートを無効に設定している場合は，インポートは実施できません。

実施方法

1. インポートファイルを「2.27.3 インポートファイルの書式と変更方法」を参照して作成し，USB メモリに保存してください。

重要

- 保存するフォルダ名またはインポートファイル名は，半角英数字のみにしてください。
- フルパスで 255 文字以下となるように，フォルダ名とファイル名を作成してください。

2. LCD タッチコンソールとインポートファイルを入れた USB メモリを，サーバシャーシのフロントパネルの USB ポートに接続してください。

   USB メモリを認識すると，LCD タッチコンソールホーム画面に「USB デバイス アンマウント」ボタンを表示します。

参考 表示しない場合は，「更新」をタッチしてください。

3. インポートを実施します。

   起動後のホーム画面で「システム構築」をタッチしてください。

4. システム構築メニュー画面で「インポート」をタッチしてください。

5. インポート(ファイル選択)画面でインポートを実施する設定ファイルをタッチし，選択してください。

   インポートファイルを選択した状態で「開く/OK」をタッチしてください。

参考

- ファイルをタッチすると背景が青に変わります。
- 画面上部にカレントディレクトリを表示していますが，画面幅を超える場合は右詰めで表示します。(左側の表示が消えていきます)

6. インポート実施の確認ダイアログを表示しますので，「はい」をタッチしてください。
7. インポート(実行)画面を表示しますので，画面が切り替わるまで待ってください。
8. 結果の表示画面を確認してください。

図 2-9 成功時の表示画面

図 2-10 失敗時の表示画面

参考 インポート失敗画面が表示された場合は,「2.27.4 インポート失敗時のトラブルシューティング」を参照してください。

9. 結果を確認後,「OK」をタッチしてください。
10. システム構築メニューを表示します。
11. USB メモリのアンマウントを実施します。
    システム構築メニューから,「USB デバイス アンマウント」ボタンをタッチしてください。

12. アンマウント実施の確認ダイアログを表示しますので，「はい」をタッチしてください。
13. システム構築メニューから，「USB デバイス アンマウント」ボタンの表示が消えていることを確認してください

14. 。USB メモリをサーバシャーシから取り外してください。
15. LCD タッチコンソールをサーバシャーシから抜去します。
    システム構築メニューから，「Logout」をタッチしてください。
16. ログアウト実施の確認ダイアログを表示しますので，「はい」をタッチしてください。
17. ログアウト画面に「LCD タッチコンソールを抜去してください」が表示することを確認してください。
18. LCD タッチコンソールをサーバシャーシから取り外してください。

(2) Web コンソールを使用する場合

Web コンソールを使用してインポートする手順を説明します。

準備するもの

- システムコンソール

実施方法

1. インポートファイルを「2.27.3 インポートファイルの書式と変更方法」を参照して作成し，システムコンソールに保存してください。

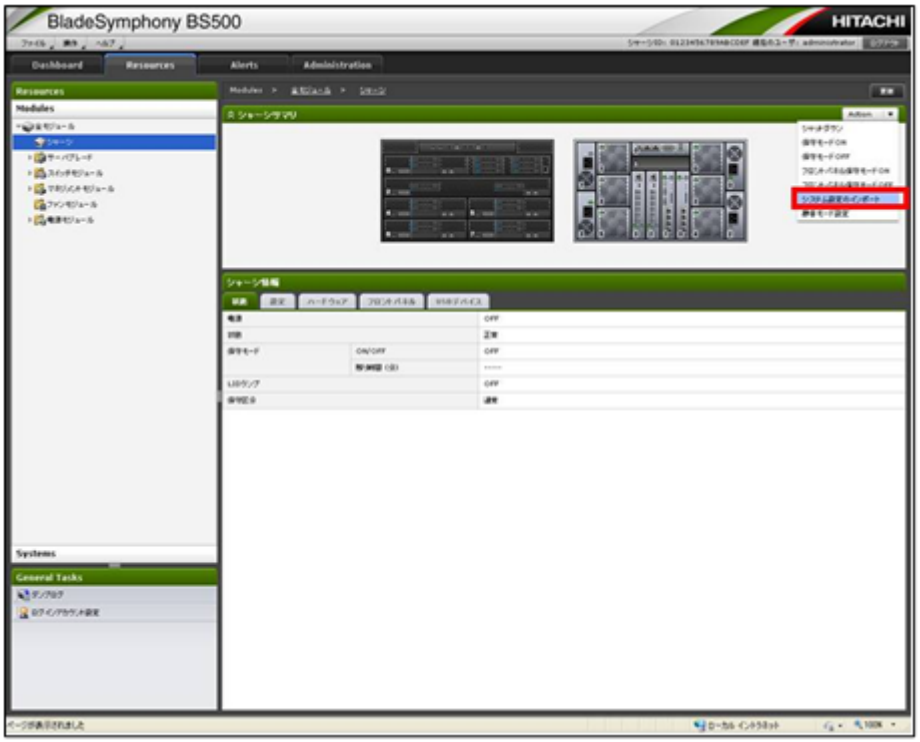
重要

- 保存するインポートファイル名は，半角英数字のみにしてください。
- インポートファイル名の長さは，200 文字以内にしてください。

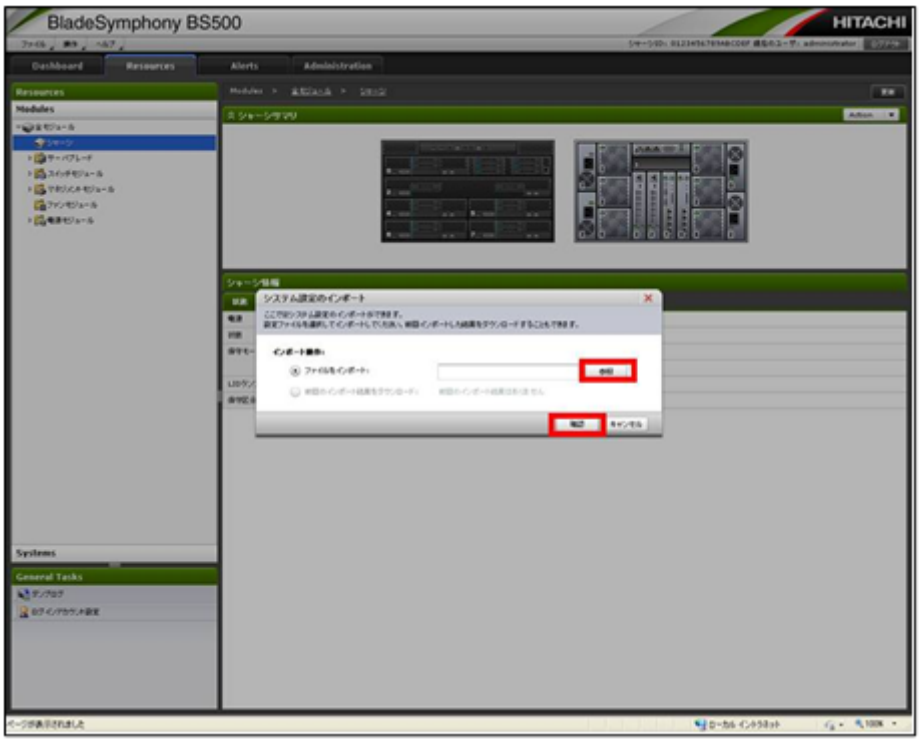
2. システムコンソール上で，マネジメントモジュールの Web コンソールへログインしてください。

重要 ログインするアカウントは，administrators ロールに所属しているアカウントでログインしてください。administrators ロールに所属しているアカウントのみ，インポートが可能です。初期アカウントの administrator は，administrators ロールに所属しています。

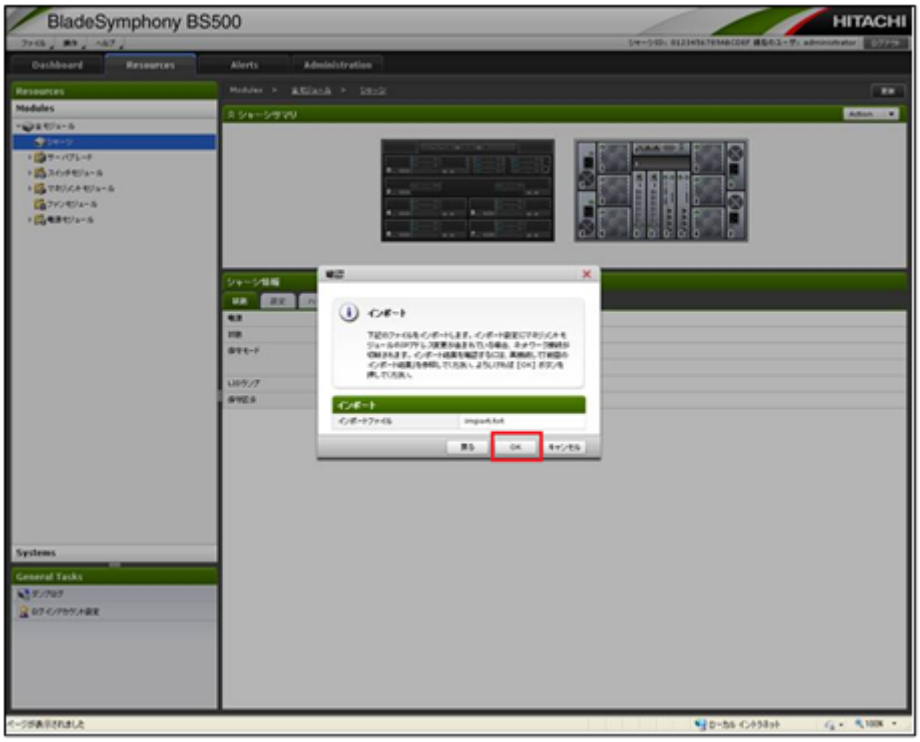
3. [Resources]タブを選択してください。
4. [Modules]のツリーにある[シャーシ]を選択してください。
5. [Action]メニューから[システム設定のインポート]を選択してください。



6. システム設定のインポートダイアログが表示されます。
   [参照]ボタンをクリックして，作成したインポートファイルを選択し，[確認]をクリックしてください。



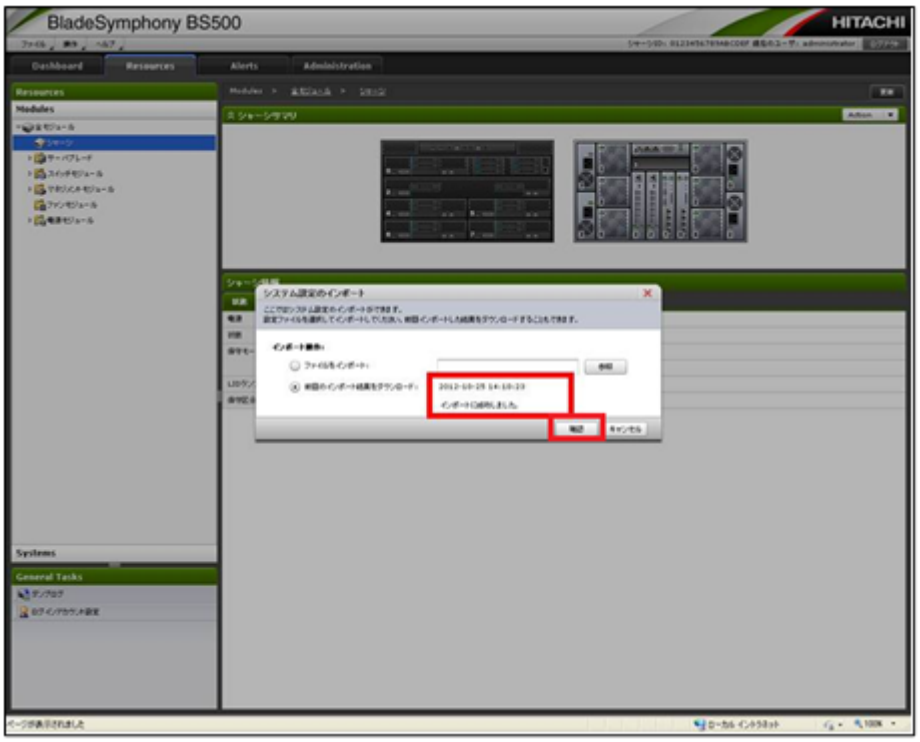
7. メッセージを確認後，[OK]ボタンをクリックしてください。



8. インポートが実行されるので，しばらく待ってください。

重要 Web コンソールで接続しているマネジメントモジュールの IP アドレスを変更するインポートの場合は，マネジメントモジュールの接続が切れます。マネジメントモジュールの Web コンソールへ再ログインして，手順 2～5 を再度実行してください。

9. インポート結果を確認し，[確認]ボタンをクリックしてください。



参考 インポート結果ファイルのダウンロードは，[前回のインポート結果をダウンロード]を選択して，[確認]ボタンをクリックしてください。

10. Web コンソールをログアウトしてください。

2.27.3 インポートファイルの書式と変更方法

『BS500 インポートファイルの雛形』を BladeSymphony Web ページの「サポート&ダウンロード」－「ドライバ・ユーティリティ ダウンロード」－「ユーティリティ（アップデートモジュール含む）」からダウンロードしてください。

Web ページ：http://www.hitachi.co.jp/products/bladesymphony/download/driver/utility.html

雛形の設定内容を変更する場合は，メモ帳などのテキストエディタでファイルを直接修正してから，USB メモリに保存してください。

参考 複数のサーバシャーシに対して個別の設定をインポートする場合は，サーバシャーシ毎にファイルを分けてください。どのサーバシャーシ用のファイルかをファイル名で区別できるようにしておくと，インポートの際に分かりやすくなります。

(1) インポートファイルの書式

ダウンロードしたインポートファイルの雛形は，以下の設定を行うファイルです。

- 時刻設定
  - タイムゾーン設定　+9:00
  - 夏時間設定　無効
- プロトコル設定

  TELNET・SSH・FTP・HTTP・HTTPS の接続許可設定

  IPv4 アドレスと IPv6 アドレスそれぞれの接続許可設定
  - 全プロトコルにおいて，全接続を許可

- HTTP に使用するポート番号：80
- HTTPS に使用するポート番号：443

・ ネットワーク設定

マネジメントモジュールの IP アドレス設定

- IP アドレス：192.168.0.1
- サブネットマスク：255.255.255.0
- デフォルトゲートウェイ：0.0.0.0
- DNS サーバアドレス：0.0.0.0

マネジメントモジュールの IPv6 アドレス設定

- IP アドレス：0000:0000:0000:0000:0000:0000
- プレフィックス：128
- デフォルトゲートウェイ：0000:0000:0000:0000:0000:0000
- DNS サーバアドレス：0000:0000:0000:0000:0000:0000

サーバブレードの IP アドレス設定　※全サーバブレード

- IP アドレス：0.0.0.0
- サブネットマスク：0.0.0.0
- デフォルトゲートウェイ：0.0.0.0

サーバブレードの IPv6 アドレス設定　※全サーバブレード

- IP アドレス：0000:0000:0000:0000:0000:0000
- プレフィックス：128
- デフォルトゲートウェイ：0000:0000:0000:0000:0000:0000

スイッチモジュールの IP アドレス設定　※全スイッチモジュール

- 接続種別は内部 LAN ネットワーク

次にインポートファイルの雛形(例)を示します。

```
#!header model=500

#!begin target=timezone                                                    ※1
set time timezone -z "+9:00"
set time dst -v disable
#!end

#!begin target=protocol                                                    ※2
set remote-access protocol telnet -a allow -n 0.0.0.0 -s 0.0.0.0 -a6 allow -n6 :: -p6 0
set remote-access protocol ssh -a allow -n 0.0.0.0 -s 0.0.0.0 -a6 allow -n6 :: -p6 0
set remote-access protocol ftp -a allow -n 0.0.0.0 -s 0.0.0.0 -a6 allow -n6 :: -p6 0
set remote-access protocol http -a allow -p 80 -n 0.0.0.0 -s 0.0.0.0 -a6 allow -n6 :: -p6 0
set remote-access protocol https -a allow -p 443 -n 0.0.0.0 -s 0.0.0.0 -a6 allow -n6 :: -p6 0
#!end

#!begin target=network                                                     ※3
set mgmt-module mgmt-lan -i 192.168.0.1 -s 255.255.255.0 -g 0.0.0.0 -d0 0.0.0.0 -d1 0.0.0.0
-d2 0.0.0.0
set blade mgmt-lan 0 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 1 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 2 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 3 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 4 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 5 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 6 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set blade mgmt-lan 7 -i 0.0.0.0 -s 0.0.0.0 -g 0.0.0.0
set sw-module mgmt-lan 0 -e int
set sw-module mgmt-lan 1 -e int
set sw-module mgmt-lan 2 -e int
set sw-module mgmt-lan 3 -e int
#!end

#!begin target=networkv6                                                   ※4
set mgmt-module mgmt-v6 address -st enable -i fe80::200:87ff:feb2:c24 -p 64 -gs enable -g
fe80::200:87ff:feb2:c20
set mgmt-module dns -p ipv6 -v6 fe80::200:87ff:feb2:c26,fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 0 -st enable -i fe80::200:87ff:feb2:c10 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 1 -st enable -i fe80::200:87ff:feb2:c11 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 2 -st enable -i fe80::200:87ff:feb2:c12 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 3 -st enable -i fe80::200:87ff:feb2:c13 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 4 -st enable -i fe80::200:87ff:feb2:c14 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 5 -st enable -i fe80::200:87ff:feb2:c15 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 6 -st enable -i fe80::200:87ff:feb2:c16 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
set blade mgmt-v6 address 7 -st enable -i fe80::200:87ff:feb2:c17 -p 64 -gs enable -g
fe80::200:87ff:feb2:c25
#!end
```

※1：時刻設定

※2：プロトコル設定

※3：ネットワーク設定(IPv4)

※4：ネットワーク設定(IPv6)

(2) インポートファイルの変更方法

ここでは，プロトコルとネットワークの設定変更方法(例)と，制限事項を説明します。インポートファイルの各設定の記述は，CLI コマンドと同一の形式となっています。設定方法の詳細は「*BladeSymphony BS500 CLI コンソール ユーザーズガイド*」を参照してください。

プロトコルの設定変更

インポートファイルに記載する，プロトコルの設定変更例を示します。

- HTTP の IPv4 ネットワーク接続を許可(無制限)にする

  set remote-access protocol http -a deny
- HTTP のポート番号を 80 に設定する

  set remote-access protocol http -p 80
- HTTP に接続制限をする
  - ネットワークアドレスを 192.168.0.100 に設定する
  - サブネットマスクを 255.255.255.0 に設定する

    set remote-access protocol http -n 192.168.0.100 -s 255.255.255.0

参考 HTTP ではないプロトコルの設定は HTTP を TELNET･SSH･FTP･HTTPS に変更してください。TELNET・SSH・FTP にはポート番号の設定はありません。

ネットワークの設定変更

インポートファイルに記載する，ネットワークの設定変更例を示します。

- マネジメントモジュール
  - IP アドレスを 192.168.0.1 に設定する
  - サブネットマスクを 255.255.255.0 に設定する
  - デフォルトゲートウェイを 192.168.0.100 に設定する
  - DNS サーバアドレス(1 個目)を 158.213.160.152 に設定する
  - DNS サーバアドレス(2 個目)を 158.214.50.44 に設定する
  - DNS サーバアドレス(3 個目)を 158.215.10.31 に設定する

    set mgmt-module mgmt-lan -i 192.168.0.1 -s 255.255.255.0 -g 192.168.0.100 -d0 158.213.160.152 -d1 158.214.50.44 -d2 158.215.10.31
- サーバブレード 0
  - IP アドレスを 192.168.0.10 に設定する
  - サブネットマスクを 255.255.255.0 に設定する
  - デフォルトゲートウェイを 192.168.0.100 に設定する

    set blade mgmt-lan 0 -i 192.168.0.10 -s 255.255.255.0 -g 192.168.0.100

参考 設定するサーバブレード番号を変更したい場合は 0 を 1～7 に変更してください。

- スイッチモジュール 0
  - 接続種別をマネジメントモジュールコンソール経由での接続に設定する

    set sw-module mgmt-lan 0 -e int
  - 接続種別を管理 LAN ポートから直接接続に設定する

IP アドレスを 192.168.0.31 に設定する
サブネットマスクを 255.255.255.0 に設定する
デフォルトゲートウェイを 192.168.0.100 に設定する
set sw-module mgmt-lan 0 -e mgmt -i 192.168.0.31 -s 255.255.255.0 -g 192.168.0.100

- 接続種別をスイッチモジュール外部ポートに接続に設定する
  set sw-module mgmt-lan 0 -e sw

参考 設定するスイッチモジュール番号を変更したい場合は 0 を 1～3 に変更してください。

インポートファイルを変更する際の制限事項

マネジメントモジュールファームウェア Ver：A0120 では，スイッチモジュールの設定をスイッチモジュール非搭載で実施した際にインポートに失敗します。その場合は，設定ファイルから以下の 4 行を消して，インポートを実施してください。

set sw-module mgmt-lan 0 -e int

set sw-module mgmt-lan 1 -e int

set sw-module mgmt-lan 2 -e int

set sw-module mgmt-lan 3 -e int

またインポートファイルを変更する際の制限事項として以下があります。

- 雛形に忠実に従って，変更するようにしてください。雛形に無い CLI コマンドをファイルに追加した場合や，ファイルの別の箇所にコマンドの記述を移動した場合，インポートが正しく動作しない可能性があります。
- 設定の実施をしたくないコマンドは，ファイルからコマンドを消してください。
- インポートファイルの各設定の記述は CLI コマンドになっています。詳細な設定を実施したい場合，「*BladeSymphony BS500 CLI ユーザーズガイド*」を参照してください。
- IPv6 アドレスの設定をインポートする場合は，マネジメントモジュールファームウェア Ver：A0230 以降に対して実施してください。前記バージョン以前に実施する場合は，IPv6 アドレスの設定を削除してください。

2.27.4 インポート失敗時のトラブルシューティング

インポートに失敗した場合，インポート(結果)画面に表示される失敗原因を確認してください。

(1) 「構文エラーが発生しました。」

インポートを実施したインポートファイルのコマンド文に構文エラーがあります。

1. インポートファイルを入れた USB メモリにインポート結果ファイル(importresult-yyyymmddhhmmss.txt)が保存されるので，その中身を確認してください。
   その結果ファイルの表示例は以下です。

```
E9972 : Syntax error. : (4,20) : set time timezone -s +9:00
                          (1)              (2)

E9973 : File is invalid.
```

   (1)から，インポートファイルの 4 行目の 20 文字目が間違っていることがわかります。4 行目の設定内容が(2)なので，この 20 文字目を直してください。

2. インポート結果ファイルの指摘箇所から，インポートファイルを作成し直し，再度インポートを実施してください。

(2) 「実行に失敗しました。」

インポートを実施したインポートファイルのコマンドが不可能な設定内容になっている等の要因で，失敗しています。

1. インポートファイルを入れた USB メモリにインポート結果ファイル(importresult-yyyymmddhhmmss.txt)が保存されるので，その中身を確認してください。
   その結果ファイルの表示例は以下です。

   $ #!begin target=network

   $ set mgmt-module mgmt-lan -i 192.168.0.100 -s 255.255.255.0 -g 192.168.0.200 -d0 192.168.0.101 -d1 192.168.0.102 -d2 192.168.0.103

   I0001 : Setting was completed.

   S0002 : Command succeeded.

   S0000 : Command was finished.

   $ set blade mgmt-lan 0 -i 192.168.0.301 -s 255.255.255.0 -g 0.0.0.0-(1)

   E0001 : Command was canceled. Parameter was invalid.-(2)

   S0005 : Command was invalid.-(3)

   S0000 : Command was finished.

   (2)，(3)が表示されたコマンド文((1))の内容を確認してください。(2)には「Command was canceled.」の後にその間違いの原因が書かれています。

2. インポート結果ファイルの指摘箇所から，インポートファイルを作成し直し，再度インポートを実施してください。

(3) 「結果出力ファイルの書き込みに失敗しました。」

インポートファイルを入れた USB メモリにインポート結果ファイル(importresult-yyyymmddhhmmss.txt)を書き込む際に失敗しました。

1. USB メモリがサーバシャーシに挿入されていることを確認してください。また，USB メモリの空き容量を確認してください。
   インポート結果ファイルは最大 5KB のファイルになります。

(4) 「指定されたファイルが見つかりません。」

1. インポートを実施する際に指定したインポートファイルを入れたUSBメモリが，サーバシャーシに挿入されていることを再度確認し，インポートを実施してください。

(5) 「予期せぬエラーが発生しました。」

インポートを実施する制御系でエラーが発生しているため，下記お問い合わせ先まで連絡してください。

お問い合わせ先

下記Webページに記載のＨＣＡセンタまで連絡してください。

http://www.hitachi.co.jp/products/bladesymphony/download/driver/utility.html#toiawase

参考 その他のメッセージが出た場合も，ＨＣＡセンタまで連絡してください。

2.28 ログ

マネジメントモジュールとサーバブレードが出力するログについて説明します。

2.28.1 マネジメントモジュールから参照可能なログ

マネジメントモジュールから，次のログが参照可能です。

表 2-141 マネジメントモジュールから参照可能なログ

項目	内容
システムイベントログ	システムイベントログ(SEL)を表示します。システム装置に発生した情報，警告，障害のイベントが記録されています。
Additional WWN 変更ログ	Additional WWN の変更の履歴です。詳細は「2.10.8 additional WWN, additional MAC アドレスの変更ログ」を参照してください。
Additional MAC アドレス変更ログ	Additnonal MAC アドレスの変更の履歴です。詳細は「2.10.8 additional WWN, additional MAC アドレスの変更ログ」を参照してください。
MAR ログ	MAR ログを表示します。MAR は Maintenance Action Report の略で，障害通報の要因となった事象が記録されています。
操作ログ／監査ログ	マネジメントモジュール，BMC への操作の履歴です。詳細は「2.28.3 操作ログ／監査ログ」を参照してください。
環境ログ	システムの入排気温度の履歴です。
ダンプログ	システム装置のダンプログを保存します。ダンプログには，システム装置の各種設定，ログ，障害解析用の内部データが含まれています。詳細は「2.28.2 ダンプログ」を参照してください。

表 2-142 Web コンソールでの操作方法

項目	画面
システムイベントログ	Alerts タブ → All Logs → システムイベントログ
Additional WWN 変更ログ	Alerts タブ → All Logs → Additional WWN 変更ログ
Additional MAC アドレス変更ログ	Alerts タブ → All Logs → Additional MAC 変更ログ
MAR ログ	Alerts タブ → All Logs → MAR ログ

項目	画面
操作ログ／監査ログ	Alerts タブ → All Logs → 操作ログ
環境ログ	Alerts タブ → All Logs → 環境ログ
ダンプログ	General Tasks → ダンプログ

表 2-143 CLI コンソールでの操作方法

項目	コマンド
システムイベントログ	show log sel
Additional WWN 変更ログ	show log wwn-edit
Additional MAC アドレス変更ログ	show log mac-edit
MAR ログ	show log mar-log
環境ログ	show log environment
ダンプログ	export log failure

表 2-144 LCD タッチコンソールでの操作方法

項目	画面
ダンプログ	ダンプログ採取

2.28.2 ダンプログ

ダンプログには，システム装置の各種設定，ログ，障害解析用の内部データが含まれています。システム装置に何らかの問題が発生した場合は，ダンプログを採取して，お買い求め先または保守員にお問い合わせください。

ダンプログはファイルの形式となっており，tar アーカイブされています。展開すると次のようなファイルが生成されます。

- raslogA-YYYYMMDD-hhmmss.tar.gz
- svpsts_ja-YYYYMMDD-hhmmss.gz
- svpsts_en-YYYYMMDD-hhmmss.gz
- hvmdumpA-YYYYMMDD-hhmmss.tar
- trc-YYYYMMDD-hhmmss.tar.gz
- marlog-YYYYMMDD-hhmmss.tar
- oplog_svp-YYYYMMDD-hhmmss.dmp

その他，障害解析用のファイルが存在することがあります。

svpsts_ja-YYYYMMDD-hhmmss.gz，svpsts_en-YYYYMMDD-hhmmss.gz には，次の内容が記録されています。

- ダンプログ採取時点の System Event Log
- ダンプログ採取時点の機器構成
- ダンプログ採取時点の主要なユーザ設定内容

これらのファイルは，gzip 圧縮されているため，解凍後テキストエディタで参照してください。svpsts_ja は日本語，svpsts_en は英語のファイルとなります。

参考

- tar アーカイブの解凍，gzip 圧縮の解凍は，一般の解凍ソフトを使用して実施してください。
- svpsts_ja-YYYYMMDD-hhmmss.gz, svpsts_en-YYYYMMDD-hhmmss.gz 以外のファイルは障害解析用のログです。内部フォーマットは開示しておりません。
- hvmdumpA-YYYYMMDD-hhmmss.tar は，HVM がマネジメントモジュールに保存するダンプログです。HVM は，障害発生時に自動的に HVM ダンプログを保存します。また，HVM ダンプは，障害解析用に手動で保存することができます。手動で保存するには，HVM スクリーンや HvmSh を使用する必要があります。
- 【マネジメントモジュールファームウェアバージョン A0145 以降】
  指定したサーバブレードの HVM 稼働時ダンプログを採取することができます。詳細は「2.19.24 HVM 稼働時ダンプの採取」を参照してください。
  この HVM 稼働時ダンプログは，ファイルとしてダウンロードすることができますが，マネジメントモジュールには保存されません。

(1) ダンプログ取得方法

マネジメントモジュールの Web コンソールからダンプログを採取する際の実施例は，次の通りです。

1. DashBoard タブで，右下のシステムイベントログのダンプログボタンを押します。
2. DashBoard タブ以外のタブで，左下の General Tasks のダンプログボタンを押します。

ログは Web コンソールを接続している PC 上に保存されます。

保存場所は画面の指示に従って指定してください。

重要 Web ブラウザのインターネットのオプション設定のポップアップブロックは，無効にしておいてください。ダンプログを採取し終わった後に，ポップアップが出ますが，ブロックを有効にしていると，ポップアップが出ないため，ダンプログの取得に失敗します。

2.28.3 操作ログ／監査ログ

操作ログ／監査ログは，システム装置に対する操作を記録したログです。マネジメントモジュールの操作とサーバブレードの操作のうち，「2.28.4 操作ログ／監査ログメッセージ一覧」に示した操作が記録されます。

重要

- マネジメントモジュールを非冗長構成でご使用になる場合，マネジメントモジュールを交換すると，それまで記録していたマネジメントモジュールの操作ログ／監査ログが失われます。
- サーバブレードを交換すると，それまで記録していたサーバブレードの操作ログ／監査ログが失われます。
- 操作ログ／監査ログのメッセージはファームウェアのバージョンによって変わることがあります。

操作ログ／監査ログの諸元は次のとおりです。

表 2-145 操作ログ／監査ログの諸元

分類	サーバブレード操作ログ／監査ログ	マネジメントモジュール操作ログ／監査ログ
記録方法	操作イベントをカテゴリに分類し成功・失敗・発生を記録	
記録範囲	装置の起動・停止操作，認証操作，設定変更操作，保守操作を記録 （記録する操作内容は「2.28.4 操作ログ／監査ログメッセージ一覧」を参照してください）	
記録件数	最大 2048 件／サーバブレード ※各々記録件数上限に到達した場合は最古の操作記録から上書きします。	サーバブレード権限で実行可能な操作：最大 2048 件／サーバブレード 上記以外の操作：最大 2048 件 ※各々記録件数上限に到達した場合は最古の操作記録から上書きします。

分類	サーバブレード操作ログ／監査ログ	マネジメントモジュール操作ログ／監査ログ
ダウンロード方法	マネジメントモジュールのコンソールから実施 形式：可変長 CSV ファイル(区切り文字：「,」) 文字コード：Shift-JIS	
ダウンロード件数	最大 2048 件	サーバブレード選択時：最大 2048 件 サーバシャーシ選択時：最大 18432 件 (サーバブレード各 2048 件×8 サーバブレード＋サーバブレード以外 2048 件)

操作ログのフォーマットは次のとおりです。なお，マネジメントモジュールとサーバブレードでログのフォーマットは同一です。

表 2-146 操作ログのフォーマット

項目名	サイズ	項目説明	備考
シーケンス番号(seq_no)	1～10	ログ内での順序を識別するための番号を記録します。 1～9999999999 の範囲で番号を付け，9999999999 を超えると 1 に戻ります。	－
日付・時刻(date)	29	操作を記録した日時，タイムゾーンを記録します。 YYYY-MM-DDThh:mi:ss.SSS±h2:s2 YYYY:西暦年，MM:月，DD:日， T:固定(区切り)，hh:時，mi:分，ss:秒，SSS:ミリ秒(000 固定)，h2:タイムゾーンオフセット時※，m2:タイムゾーンオフセット分※ ※タイムゾーンは UTC とのオフセットを記録しています。	－
サーバブレード番号(par_no)	1	• サーバブレード操作ログ： 操作イベントが発生したサーバブレード番号を記録します。 • マネジメントモジュール操作ログ： サーバブレード権限で実行可能な操作：サーバブレード番号 0～7 を記録します。上記以外の操作：8 を記録します。	サーバブレード権限のユーザでログインした場合は，そのユーザが操作可能なサーバブレードを操作した記録のみを提供します。
装置名称(compid)	7～17	操作を行った装置の名称を記録します。 • サーバブレード操作ログ： Server Blade • マネジメントモジュール操作ログ： Management Module	－
発生場所(place)	15～40	操作を行った装置のホスト名を記録します。 • サーバブレード操作ログ： サーバブレードの IP アドレス • マネジメントモジュール操作ログ： マネジメントモジュールの IP アドレス	－
操作種別(categ)	7～19	操作内容を分類したカテゴリ名を記録します。	「表 2-146 操作イベント種別表」を参照してください。

項目名	サイズ	項目説明	備考
操作結果(result)	7～10	操作の結果を記録します。(成功／失敗／発生)	「表 2-147 操作イベント結果表」を参照してください。
操作者分類(subjtype)	10～14	操作を行った対象の分類を記録します。 ・ ユーザー操作：「User Operation」 ・ システムプロセスによる操作：「System Process」	－
操作者(subject)	1～32	操作を行った対象者を記録します。 ・ ユーザ操作：ログインアカウント名 ・ システムプロセスによる操作：プロセス識別子	－
セッション ID(sessionid)	3～32	同一ログインアカウントで 2 名以上がログインしている場合の識別情報を記録します。(16 進)	システム処理などの該当なしの場合は「N/A」と表示します。
メッセージ ID(msgid)	4	メッセージ ID を記録します。(16 進)	－
メッセージ(message)	1～240	操作に対するメッセージを記録します。	－

参考

- 各項目は可変長で記録します。
- 各項目間の区切り文字は「,」(カンマ)で区切り，各行の終端文字は改行コード(CR，LF)です。
- メッセージは，前後をダブルクォーテーション「"」で囲い記録します。
- メッセージの文字コードは Shift-JIS で記録されます。

表 2-147 操作イベント種別表

記録内容	説明
StartStop	「起動・停止」の操作イベントを示します。
Authentication	「識別・認証」の操作イベントを示します。
ConfigurationAccess	「構成定義」の操作イベントを示します。
Maintenance	「保守」の操作イベントを示します。

表 2-148 操作イベント結果表

記録内容	説明
Success	操作イベントの成功を示します。
Failure	操作イベントの失敗を示します。
Occurrence	操作イベントの発生を示します。(成功／失敗の分類がない事象)

監査ログのフォーマットは次のとおりです。なお，マネジメントモジュールとサーバブレードでログのフォーマットは同一です。

表 2-149 監査ログのフォーマット

項目	説明	備考
統一識別子(CommonSpecID)	CELFSS 固定	－

項目	説明	備考
統一仕様リビジョン番号(Rev)	2	－
シーケンス番号(SequenceNum)	ログ内での順序を識別するための番号を記録します。1～9999999999 の範囲で番号を付けて，9999999999 を超えると 1 に戻ります。	操作ログの seq_no に対応しています。
メッセージ ID(MessageID)	メッセージ ID を記録します（16 進）。	操作ログの msgid に対応しています。
日付・時刻(DateTime)	操作を記録した日時，タイムゾーンを記録します。 YYYY-MM-DDThh:mi:ss.S±h2:m2 YYYY:西暦年，MM:月，DD:日，T:固定（区切り） hh:時，mi:分，ss:秒，S:ミリ秒（0 固定） h2:タイムゾーンオフセット時，m2:タイムゾーンオフセット分 タイムゾーンは UTC とのオフセットを記録しています。	操作ログの date に対応しています。
検出エンティティ(EntityInfo)	操作を行った装置の名称を記録します。 マネジメントモジュール監査ログ：ManagementModule	－
検出場所(Location)	操作を行った装置のホスト名を記録します。 マネジメントモジュール監査ログ：マネジメントモジュールの IP アドレス	操作ログの place に対応しています。
操作種別(Category)	操作内容を分類したカテゴリ名を記録します。	「表 2-146 操作イベント種別表」を参照してください。操作ログの categ に対応しています。
操作結果(Result)	操作の結果を記録します（成功／失敗／発生）。	Success（成功） Failed（失敗） Occurrence（発生）
操作者(SubjectID)	操作を行った対象者を記録します。 • ユーザ操作：ログインアカウント名 • システムプロセスによる操作：プロセス識別子	操作ログの subject に対応しています。
ハードウェア識別情報(HardwareID)	操作を行った装置のシリアル番号を記録します。	－
発生場所情報(LocInfo)	マネジメントモジュール監査ログ:サーバブレード権限で実行できる操作：サーバブレード番号 0～7 を記録します。上記以外の操作：8 を記録します。	サーバブレード権限のユーザでログインした場合は，そのユーザが操作できるサーバブレードの操作記録だけを提供します。操作ログの par_no に対応しています。
ロケーション識別情報(LocID)	この装置では記録しません。	－
FQDN(FQDN)	この装置では記録しません。	－
冗長化識別情報(HaID)	この装置では記録しません。	－
エージェント情報(AgentInfo)	この装置では記録しません。	－
リクエスト送信元ホスト(ReqSourceHost)	この装置では記録しません。	－

項目	説明	備考
リクエスト送信元ポート番号(ReqSourcePort)	この装置では記録しません。	－
リクエスト送信先ホスト(ReqDestHost)	この装置では記録しません。	－
リクエスト送信先ポート番号(ReqDestPort)	この装置では記録しません。	－
一括操作識別子(BatchID)	この装置では記録しません。	－
ログ種別情報(LogCateg)	この装置では記録しません。	－
アプリケーション識別情報(AppID)	この装置では記録しません。	－
予約領域(Reserv)	この装置では記録しません。	－
メッセージ(Message)	操作に対するメッセージを記録します。	操作ログの message に対応しています。

重要

- 各項目は可変長で記録します。
- 各項目間の区切り文字は「,」（カンマ）で区切り，各行の終端文字は改行コード（CR，LF）です。
- メッセージは，前後をダブルクォーテーション「"」で囲い記録します。

2.28.4 操作ログ／監査ログメッセージ一覧

マネジメントモジュールとサーバブレードの操作ログ／監査ログ一覧を次に示します。

表 2-150 マネジメントモジュールの操作ログ／監査ログメッセージ一覧

ID	操作イベント種別	採取契機	メッセージ
0802	起動・停止	マネジメントモジュールの操作指示	マネジメントモジュール N の操作を指示しました。 手段:xxx 操作内容:xxx
0803		マネジメントモジュールの操作指示の失敗	マネジメントモジュール N の操作指示に失敗しました。 手段:xxx 操作:xxx
0804		装置のシャットダウン指示	装置の電源断を指示しました。 手段:xxx
0805		装置のシャットダウン指示の失敗	装置の電源断の指示に失敗しました。 手段:xxx
0806		スイッチモジュールの操作指示	スイッチモジュール N の操作を指示しました。 手段:xxx 操作内容:xxx
0807		スイッチモジュールの操作指示の失敗	スイッチモジュール N の操作指示に失敗しました。 手段:xxx 操作:xxx
0808		サーバブレードの操作指示	サーバブレード N の操作を指示しました。 手段:xxx 操作内容:xxx
0809		サーバブレードの操作指示の失敗	サーバブレード N の操作指示に失敗しました。 手段:xxx 操作:xxx
1800	識別・認証	システムコンソールへのログイン成功	システムコンソールへのログインに成功しました。 ログインユーザー ID:xxx セッション ID:xxx 接続元 IP アドレス:xxx
1801		システムコンソールへのログイン失敗	システムコンソールへのログインに失敗しました。 ログインユーザー ID:xxx 接続元 IP アドレス:xxx 失敗要因:xxx

ID	操作イベント種別	採取契機	メッセージ
1802		システムコンソールからのログアウト	システムコンソールからのログアウトに成功しました。 ログインユーザー ID:xxx セッション ID:xxx 接続元 IP アドレス:xxx ログアウト要因:xxx
1803		Web コンソールへのログイン成功	システム Web コンソールへのログインに成功しました。 ログインユーザー ID:xxx セッション ID:xxx 接続元 IP アドレス:xxx
1804		Web コンソールへのログイン失敗	システム Web コンソールへのログインに失敗しました。 ログインユーザー ID:xxx 接続元 IP アドレス:xxx 失敗要因:xxx
1805		Web コンソールからのログアウト	システム Web コンソールからのログアウトに成功しました。 ログインユーザー ID:xxx セッション ID:xxx 接続元 IP アドレス:xxx ログアウト要因:xxx
1806		システムコンソールまたは Web コンソールへのログイン失敗	コンソールへのログインに失敗しました。 失敗要因:xxx
1810		BMC セッションの切断成功	サーバブレード xxx の BMC セッション切断に成功しました。 手段:xxx 種別:xxx 指定値:xxx
1811		BMC セッションの切断失敗	サーバブレード xxx の BMC セッション切断に失敗しました。 手段:xxx 種別:xxx 指定値:xxx
1812		パスワード期限切れ後のログイン	パスワード変更のためコンソールへのログインを許可しました。 ログインユーザー ID:xxx 理由:xxx
1814		BMC セッションの切断成功	サーバブレード xxx の BMC セッション切断に成功しました。 手段:xxx
1815		BMC セッションの切断失敗	サーバブレード xxx の BMC セッション切断に失敗しました。 手段:xxx
3803	構成定義	電源モジュールの設定変更	電源モジュールの設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3804		電源モジュールの設定変更	電源モジュール N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3806		マネジメントモジュールの管理 LAN 設定変更	管理 LAN(マネジメントモジュール)の設定が変更されました。 手段:xxx 種別:xxx 変更後:xxx
3808		スイッチモジュールの管理 LAN 設定変更	管理 LAN(スイッチモジュール xxx)の設定が変更されました。 手段:xxx 種別:xxx 変更後:xxx
3809		スイッチモジュールの管理 LAN 設定変更	管理 LAN(スイッチモジュール xxx)の設定が変更されました。 (マネジメントモジュール設定反映) 手段:xxx
380E		VLAN 設定の変更	VLAN の設定が変更されました。(ポート移動) 手段:xxx target:xxx partition:xxx switch module:xxx VLAN ID:xxx
380F		VLAN 設定の変更	VLAN の設定が変更されました。(ポート移動) 手段:xxx Target:xxx Server blade:xxx Switch module:xxx VLAN ID:xxx

ID	操作イベント種別	採取契機	メッセージ
3810		VLAN 設定の変更	VLAN の設定が変更されました。(VLAN 削除) 手段:xxx VLAN ID:xxx
3821		マネジメントモジュールの工場出荷時設定への復元の指示	マネジメントモジュール工場出荷状態への設定を指示しました。 手段:xxx 種別:xxx
3829		JP1/SC/BSM 連携設定の変更	JP1 SC/BSM 連携設定が変更されました。 (コマンドポート番号) 手段:xxx 変更後:xxx
382B		E-mail 設定の変更	E-mail の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
382E		SNMP 設定の変更	SNMP の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
382F		SNMP 設定の削除	SNMP の設定が削除されました。 手段:xxx 種別:xxx 番号:xxx
3830		セキュリティ設定の変更	xxx サービスの設定が変更されました。 手段:xxx 種別:xxx 変更後設定:xxx
3832		SSH ホスト鍵ペアの作成	SSH ホスト鍵ペアを作成しました。 手段:xxx
3834		SSH ホスト鍵ペアの保存	SSH ホスト鍵ペアをバックアップしました。 手段:xxx ファイル名:xxx
3836		SSH ホスト鍵ペアの復元	SSH ホスト鍵ペアをリストアしました。 手段:xxx ファイル名:xxx
3838		SSL 秘密鍵と自己署名証明書の生成	SSL 秘密鍵と自己署名証明書を生成しました。 手段:xxx 種別:xxx 設定内容:xxx
383A		CSR の生成	SSL 秘密鍵と証明書署名要求を生成しました。 手段:xxx 種別:xxx 設定内容:xxx
383C		証明書のインポート	証明書をインポートしました。 手段:xxx ファイル名:xxx 証明書ファイルタイプ:xxx
383E		証明書のコピー	証明書をコピーしました。 手段:xxx ファイル名:xxx 証明書ファイルタイプ:xxx
3840		証明書のバックアップ	証明書をバックアップしました。 手段:xxx ファイル名:xxx
3842		証明書のリストア	証明書をリストアしました。 手段:xxx ファイル名:xxx
3844		マネジメントモジュールの設定の保存	マネジメントモジュールの設定をバックアップしました。 手段:xxx ファイル名:xxx
3845		マネジメントモジュールの設定の復元	マネジメントモジュールの設定のリストアを指示しました。 手段:xxx ファイル名:xxx
384B		LDAP 設定の変更	LDAP の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
384C		LDAP 設定の変更	LDAP の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx
3850		省電力設定の変更	省電力設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3853		省電力設定の変更	サーバブレード N の省電力設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
385A		時刻の変更	マネジメントモジュールの時刻設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx

ID	操作イベント種別	採取契機	メッセージ
3861		N+M コールドスタンバイによるサーバブレード情報設定変更	サーバブレード N で N+M コールドスタンバイのサーバブレード情報を設定しました。 手段:xxx
3862		サーバブレードの設定変更	サーバブレード N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3863		サーバブレードの設定変更	サーバブレード N の設定が変更されました。 手段:xxx 種別:xxx
3864		サーバブレードの管理 LAN 設定変更	管理 LAN(サーバブレード N)の設定が変更されました。 手段:xxx 種別:xxx 変更後:xxx
3867		Additional WWN の設定変更	AdditionalWWN の設定が変更されました。 手段:xxx サーバブレード番号:xxx
3868		Additional WWN の設定変更	AdditionalWWN の設定が変更されました。 手段:xxx サーバブレード番号:xxx カード種別:xxx スロット番号:xxx
3869		Additional WWN の設定変更	AdditionalWWN の設定を初期化しました。 手段:xxx サーバブレード番号:xxx
386A		Additional WWN の設定変更	AdditionalWWN の設定を初期化しました。 手段:xxx サーバブレード番号:xxx カード種別:xxx スロット番号:xxx
386B		Additional MAC アドレスの設定変更	AdditionalMAC の設定が変更されました。 手段:xxx サーバブレード番号:xxx
386C		Additional MAC アドレスの設定変更	AdditionalMAC の設定が変更されました。 手段:xxx サーバブレード番号:xxx カード種別:xxx スロット番号:xxx
386D		Additional MAC アドレスの設定変更	AdditionalMAC の設定を初期化しました。 手段:xxx サーバブレード番号:xxx
386E		Additional MAC アドレスの設定変更	AdditionalMAC の設定を初期化しました。 手段:xxx サーバブレード番号:xxx カード種別:xxx スロット番号:xxx
3870		サーバブレードの工場出荷時設定への復元	サーバブレード N 工場出荷状態に設定しました。 手段:xxx 種別:xxx
3872		N+M コールドスタンバイテストアラート発行	サーバブレード N JP1/SC/BSM 連携テストアラートを送信しました。(N+M cold standby) 手段:xxx 種別:xxx
3873		サーバブレードの設定のバックアップ	サーバブレード N の設定(xxx)をバックアップしました。 手段:xxx バックアップ時刻:xxx ファイル名:xxx
3874		サーバブレードの設定のリストア	サーバブレード N の設定(xxx)をリストアしました。 手段:xxx バックアップ時刻:xxx
3875		サーバブレードのバックアップデータの削除	サーバブレード N の設定(xxx)を削除しました。 手段:xxx
3876		サーバブレードの設定(HBA)のバックアップ	サーバブレード N の設定(xxx)をバックアップしました。 手段:xxx 種別:xxx スロット番号:xxx バックアップ時刻:xxx ファイル名:xxx
3877		サーバブレードの設定(HBA)のリストア	サーバブレード N の設定(xxx)をリストアしました。 手段:xxx 種別:xxx スロット番号:xxx バックアップ時刻:xxx
3878		サーバブレードのバックアップデータ(HBA)の削除	サーバブレード N の設定(xxx)を削除しました。 手段:xxx 種別:xxx スロット番号:xxx

ID	操作イベント種別	採取契機	メッセージ
3879		サーバブレードの設定のバックアップ	サーバブレード N の設定(xxx)をバックアップしました。 手段:xxx ファイル名:xxx
387A		サーバブレードの設定のリストア	サーバブレード N の設定(xxx)をリストアしました。 手段:xxx ファイル名:xxx
387D		サーバブレードの設定のバックアップ	サーバブレード N の設定(xxx)をバックアップしました。 手段:xxx 種別:xxx スロット番号:xxx
387E		サーバブレードの設定のリストア	サーバブレード N の設定(xxx)をリストアしました。 手段:xxx 種別:xxx スロット番号:xxx
387F		サーバブレードの設定の削除	サーバブレード N の設定(xxx)を削除しました。 手段:xxx 種別:xxx スロット番号:xxx
3880		アカウントの追加	アカウントが追加されました。 手段:xxx アカウント:xxx ステータス:xxx ロール:xxx
3881		アカウントの変更	アカウントが変更されました。 手段:xxx アカウント:xxx ステータス:xxx ロール:xxx
3882		アカウントの削除	アカウントが削除されました。 手段:xxx アカウント:xxx
3883		ロールの変更	ロールが変更されました。 手段:xxx ロール:xxx P0123567:xxx SW0123:xxx Net:xxx Chassis:xxx Account:xxx
3884		ロールの追加	ロールが追加されました。 手段:xxx ロール:xxx P0123567:xxx SW0123:xxx Net:xxx Chassis:xxx Account:xxx
3885		ロールの削除	ロールが削除されました。 手段:xxx ロール:xxx
3888		JP1/SC/BSM 連携設定の追加	JP1/SC/BSM 連携設定が追加されました。 手段:xxx サーバ:xxx IP アドレス:xxx アラートポート番号:xxx アラートレベル:xxx リトライ間隔:xxx リトライ継続時間:xxx
3889		JP1/SC/BSM 連携設定の変更	JP1/SC/BSM 連携設定が変更されました。 手段:xxx サーバ:xxx 種別:xxx 変更後:xxx
388A		JP1/SC/BSM 連携設定の削除	JP1/SC/BSM 連携設定が削除されました。 手段:xxx サーバ:xxx
388E		JP1/SC/BSM 連携設定の変更	JP1/SC/BSM 連携設定が変更されました。 手段:xxx サーバ:xxx
3890		E-mail 設定(宛先)の追加	E-mail の宛先が追加されました。 手段:xxx
3891		E-mail 設定(宛先)の変更	E-mail の宛先が変更されました。 手段:xxx
3892		E-mail 設定(宛先)の削除	E-mail の宛先が削除されました。 手段:xxx
3898		スイッチモジュールの設定変更	スイッチモジュール N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3899		スイッチモジュールの設定変更	スイッチモジュール N の設定が変更されました。 手段:xxx ポート番号:xxx 種別:xxx 変更内容:xxx 変更後:xxx
389A		LCD タッチコンソールの暗証番号の変更	LCD タッチコンソールの暗証番号が変更されました。 手段:xxx
389B		LCD タッチコンソールの暗証番号の初期化	LCD タッチコンソールの暗証番号が初期化されました。 手段:xxx

ID	操作イベント種別	採取契機	メッセージ
389D		サーバブレードホスト情報のクリア	サーバブレード N のホスト情報がクリアされました。 手段:xxx
3900		HCSM コマンドによる HCSM 連携機能設定変更	HCSM 連携設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3901		HCSM コマンドによる HCSM サーバ設定追加	HCSM 管理サーバ設定が追加されました。 手段:xxx IP アドレス:xxx アラートポート番号:xxx アラートレベル:xxx リトライ間隔:xxx リトライ継続時間:xxx
3902		HCSM コマンドによる HCSM サーバ設定変更	HCSM 管理サーバ設定が変更されました。 手段:xxx IP アドレス:xxx 種別:xxx 変更前:xxx 変更後:xxx
3903		HCSM コマンドによる HCSM サーバ設定変更	HCSM 管理サーバ設定が変更されました。 手段:xxx IP アドレス:xxx 変更内容:xxx 変更後:xxx
3904		HCSM コマンドによる HCSM サーバ設定削除	管理サーバ設定が削除されました。 手段:xxx IP アドレス:xxx
3905		HCSM コマンドによる HCSM サーバセッション切断	HCSM 管理サーバが切断されました。 手段:xxx IP アドレス:xxx
3910		マネジメントモジュールのセキュリティ強度設定の変更	マネジメントモジュールのセキュリティ強度設定が変更されました。 手段:XXX 変更内容:XXX 変更後:XXX
3911		サーバブレードのセキュリティ強度設定の変更	サーバブレード N のセキュリティ強度設定が変更されました。 手段:XXX 変更内容:XXX 変更後:XXX
3912		マネジメントモジュールの TLS/SSL バージョン設定の変更	マネジメントモジュールの TLS/SSL バージョン設定が変更されました。 手段:XXX 変更内容:XXX 変更後:XXX
391A		ログインバナー設定の変更	ログインバナー設定が変更されました。 手段:xxx 変更後:xxx
391B		ログインバナーメッセージの登録	ログインバナーメッセージが登録されました。 手段:xxx
391C		ログインバナーメッセージの変更	ログインバナーメッセージが変更されました。 手段:xxx
391D		ログインバナーメッセージの削除	ログインバナーメッセージが削除されました。 手段:xxx
391E		Web コンソール(管理 LAN)設定の変更	Web コンソール(管理 LAN)設定が変更されました。 手段:xxx 変更後:xxx
391F		Web コンソール(保守 LAN)設定の変更	Web コンソール(保守 LAN)設定が変更されました。 手段:xxx 変更後:xxx
392B		パスワードポリシー設定の変更	パスワードポリシー設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
392C		BMC ユーザアカウント設定の変更	BMC ユーザアカウントが変更されました。 手段:xxx サーバブレード番号:xxx アカウント番号:xxx 使用:xxx ユーザ名:xxx
392D		IPMI ユーザアカウント設定の変更	IPMI ユーザアカウントが変更されました。 手段:xxx サーバブレード番号:xxx アカウント番号:xxx 使用:xxx ユーザ名:xxx 権限:xxx
392E		フロントパネル USB 設定の変更	USB 設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx

ID	操作イベント種別	採取契機	メッセージ
392F		認証情報暗号化設定変更	認証情報暗号化設定が変更されました。 手段:xxx 変更後:xxx
3930		サーバブレードの設定変更	サーバブレード N の設定が変更されました。 手段:xxx 種別:xxx NIC 指定:xxx 冗長化:xxx
3931		RADIUS の設定変更	RADIUS の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3932		RADIUS サーバの設定変更	RADIUS サーバ N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
393A		SVP-HVM 管理通信設定の変更	マネジメントモジュールーHVM 間の通信設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
393B		サーバブレードの設定変更	サーバブレード N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
393C		サーバブレードの設定変更	サーバブレード N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
393D		サーバブレードの設定変更	サーバブレード N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
3944		HCSM コマンドによる HCSM サーバ設定変更	HCSM 管理サーバ設定が変更されました。 手段:xxx IP アドレス:xxx 変更内容:xxx 変更後:xxx
3950		RADIUS サーバの設定変更	RADIUS サーバ N の設定が変更されました。 手段:xxx 種別:xxx 変更内容:xxx 変更後:xxx
8800	保守	サーバシャーシを通常モードから保守モードに移行	サーバシャーシを通常モードから保守モードに変更しました。 手段:xxx
8801		サーバシャーシを保守モードから通常モードに移行	サーバシャーシを保守モードから通常モードに変更しました。 手段:xxx
8802		サーバブレードを通常モードから保守モードに移行	サーバブレード N を通常モードから保守モードに変更しました。 手段:xxx
8803		サーバブレードを保守モードから通常モードに移行	サーバブレード N を保守モードから通常モードに変更しました。 手段:xxx
8804		スイッチモジュールを通常モードから保守モードに移行	スイッチモジュール N を通常モードから保守モードに変更しました。 手段:xxx
8805		スイッチモジュールを保守モードから通常モードに移行	スイッチモジュール N を保守モードから通常モードに変更しました。 手段:xxx
8806		マネジメントモジュールを通常モードから保守モードに移行	マネジメントモジュール N を通常モードから保守モードに変更しました。 手段:xxx
8807		マネジメントモジュールを保守モードから通常モードに移行	マネジメントモジュール N を保守モードから通常モードに変更しました。 手段:xxx
8808		フロントパネルを通常モードから保守モードに移行	フロントパネルを通常モードから保守モードに変更しました。 手段:xxx
8809		フロントパネルを保守モードから通常モードに移行	フロントパネルを保守モードから通常モードに変更しました。

ID	操作イベント種別	採取契機	メッセージ
			手段:xxx
8810		サーバブレードファームウェアの更新の指示	サーバブレード N のファームウェアの更新を指示しました。 手段:xxx
8811		HVM ファームウェアの更新の指示	HVM ファームウェアの更新を指示しました。 手段:xxx バンク番号:xxx （※1）
8812		HVM ファームウェアの削除の指示	HVM ファームウェアの削除を指示しました。 手段:xxx バンク番号:xxx （※1）
8813		スイッチモジュールファームウェアの更新の指示	スイッチモジュール N のファームウェアの更新を指示しました。 手段 xxx
8814		マネジメントモジュールファームウェアの更新の指示	マネジメントモジュールファームウェアの更新を指示しました。 手段:xxx
8815		マネジメントモジュールファームウェアの更新の指示	マネジメントモジュールファームウェアの更新(Copy and Update)を指示しました。 手段:xxx
8819		サーバブレードへ iso イメージファイルのマウント	サーバブレード N iso イメージファイルをマウントしました。 手段:xxx ファイル名:xxx
881A		サーバブレードから iso イメージファイルのアンマウント	サーバブレード N iso イメージファイルをアンマウントしました。 手段:xxx ファイル名:xxx
881C		EFI 時刻合わせ機能設定の変更	サーバブレード xxx の EFI 時刻合わせ設定が変更されました。 手段:xxx 変更後:xxx

（※1）：バンク番号は，面の番号のことを示します。詳細は「2.19.22 HVM ファームウェアのアップデート」を参照してください。

表 2-151 サーバブレードの操作ログ／監査ログメッセージ一覧

ID	操作イベント種別	採取契機	メッセージ
1001	識別・認証	リモートコンソールへのログイン成功	リモートコンソールへのログインに成功しました。 ユーザ名：xxx 接続元 IP アドレス：xxx ユーザ認証方式：xxx
1002		リモートコンソールからのログアウト	リモートコンソールからログアウトしました。 ユーザ名：xxx 接続元 IP アドレス：xxx 要因：xxx
1003		リモートコンソールへのログイン失敗	リモートコンソールへのログインに失敗しました。 ユーザ名：xxx 接続元 IP アドレス：xxx 要因：xxx
1008		サーバブレード Web コンソールへのログイン成功	サーバブレード Web コンソールへのログインに成功しました。 ユーザ名：xxx 接続元 IP アドレス：xxx ユーザ認証方式：xxx
1009		サーバブレード Web コンソールからのログアウト	サーバブレード Web コンソールからログアウトしました。 ユーザ名：xxx 接続元 IP アドレス：xxx 要因：xxx
100A		サーバブレード Web コンソールへのログイン失敗	サーバブレード Web コンソールへのログインに失敗しました。 ユーザ名：xxx 接続元 IP アドレス：xxx 要因：xxx

2.29 ファームウェア

マネジメントモジュールとサーバブレードの，ファームウェアのアップデートについて説明します。

2.29.1 マネジメントモジュールからアップデート可能なファームウェア

ファームウェアとは，ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェアのことです。本システム装置においても複数のファームウェアが組み込まれています。マネジメントモジュールからは，次のファームウェアのアップデートが可能です。

表 2-152 ファームウェアの種類

名称	内容
マネジメントモジュールファームウェア	マネジメントモジュール上で動作するファームウェアです。
辞書	マネジメントモジュール上に格納されている，ログのメッセージ変換を行うデータファイルです(※1)。
装置パラメータ	マネジメントモジュール上に格納されている，システム装置に搭載されるモジュールのハードウェアに設定する各種パラメータなどを定義するためのデータファイルです(※1)。
サーバブレードファームウェア	サーバブレード上で動作するファームウェアです。BMC と UEFI が含まれます。
HVM ファームウェア	サーバブレード上で HVM を稼働させるために動作するファームウェアです。 HVM ファームウェアのアップデート手順については，「2.19.22 HVM ファームウェアのアップデート」を参照してください。

※1：これらは厳密にはファームウェアではないですが，ファームウェアと同様にマネジメントモジュールからアップデートを行うものなので，便宜上本表に記載しています。

2.29.2 マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート

マネジメントモジュールファームウェア，辞書，装置パラメータのアップデートは，マネジメントモジュールのコンソールまたは HCSM(Ver7.5 以降)から実施でき，一括でアップデートすることができます。

表 2-153 アップデート対象一覧

アップデート対象	所要時間(分)	マネジメントモジュールリブート有無	システム稼働中の実施可否
マネジメントモジュールファームウェア	25～30	有(※1)	可(※2)
辞書	5～10	無	可
装置パラメータ	5～10	無	可

※1：マネジメントモジュールファームウェアのアップデートを実施すると，マネジメントモジュールが自動的にリブートします。マネジメントモジュールが冗長化されているときは，まず主系のマネジメントモジュールがリブートし，元々待機系だったマネジメントモジュールが主系となります。その後，リブートしたマネジメントモジュールの起動が完了すると，もう 1 台のマネジメントモジュールがリブートし，元々主系だったマネジメントモジュールが主系に戻ります。

※2：システム稼働中にアップデートを実施する際には注意事項があるため，必ず「マネジメントモジュールファームウェアアップデート時の制限事項」をお読みになってから，実施してください。

マネジメントモジュールファームウェアアップデート時の制限事項

マネジメントモジュールファームウェアのアップデートを行う場合，次の制限事項があります。

【マネジメントモジュールが非冗長構成の場合】

マネジメントモジュールが非冗長構成の時は，全サーバブレードを電源 OFF してからマネジメントモジュールのアップデートを実施してください。

【マネジメントモジュールが冗長構成の場合】

マネジメントモジュールが冗長構成の時は，サーバブレードの稼働中にマネジメントモジュールのファームアップデートが可能ですが，次の制限事項がありますので必ずご確認の上，リスクをご了承いただいた上で実施してください。

- マネジメントモジュールファームウェア，辞書，装置パラメータのいずれかのアップデートもしくは，複数の同時アップデートを実施している最中に，別コンソールもしくは HCSM からマネジメントモジュールファームウェア，辞書，装置パラメータのいずれかのアップデートもしくは，複数の同時アップデートを実施しないでください。
  - 実施した場合，アップデートに失敗する可能性があります。アップデートに失敗した場合は，再度アップデートを実施してください。
  - マネジメントモジュールファームウェアのバージョンが A0145 以前で，マネジメントモジュールが冗長構成の場合は，アップデートに失敗するだけでなく，待機系マネジメントモジュールが障害となる可能性があります。

    障害となった場合は，お買い求め先か，保守員に連絡してください。
- バージョンアップ作業中は，マネジメントモジュール動作が一時中断するため，該当システム装置で次の表に記載の操作は行わないでください。これらの操作を行った場合，ネットワーク接続が一時的に切断されることにより，操作が失敗する場合があります。マネジメントモジュールファームウェアのバージョンアップ作業終了後，再度操作を実施してください。

表 2-154 バージョンアップ作業中の禁止事項

バージョンアップ作業中の禁止事項
N+M コールドスタンバイの手動切替および復帰操作(本操作を失敗した場合，回復のために N+M 環境の再構築が必要となる場合があります)
マネジメントモジュールコンソールへのログイン
JP1/ServerConductor/Blade Server Manager の操作
JP1/ServerConductor/Deployment Manager の操作
JP1/ServerConductor/Control Manager の操作
JP1/Cm2/Network Node Manager の操作
HCSM の操作
HA モニタ クラスタ構成の構築･変更
リモートコンソールの使用
HVM の操作
サーバブレードファームウェアのアップデート
HVM ファームウェアのアップデート

- サーバブレードもしくはシステム装置の電源 ON 実行中や電源 OFF 実行中に，マネジメントモジュールファームウエアのバージョンアップ作業を行うと正常に行われない可能性があります。該当システム装置に対する次の操作を行わないでください。

表 2-155 電源 ON 実行中や電源 OFF 実行中の禁止事項

電源 ON 実行中や電源 OFF 実行中の禁止事項
サーバブレード，サーバシャーシの電源 OFF/ON 操作（スケジュール運転による操作も含む）

- バージョンアップ作業中，JP1/ServerConductor/Blade Server Manager へ次のアラートが報告される場合があります。（本アラートは作業手順の中で確認するものであり，システム動作には影響ありません）

表 2-156 アラート

種類	内容
警告	0x17A0 LAN ポート<Management LAN port0>の冗長性がありません。
	0x17A0 LAN ポート<Management LAN port1>の冗長性がありません。
	0x17A0 LAN ポート<Maintenance LAN port>の冗長性がありません。
インフォメーション	0x17A1 LAN ポート<Management LAN port0>の冗長性が回復しました。
	0x17A1 LAN ポート<Management LAN port1>の冗長性が回復しました。
	0x17A1 LAN ポート<Maintenance LAN port>の冗長性が回復しました。

※上記以外の「インフォメーション」アラートが報告される場合がありますが，システム動作には影響ありません。

- バージョンアップ作業中，HCSM へ次のアラートが報告される場合があります。（本アラートは作業手順の中で確認するものであり，システム動作には影響ありません）

表 2-157 アラート

種類	内容
警告	FD78h モジュールの冗長性がなくなりました。(指摘部位：Management LAN Port0)
	FD78h モジュールの冗長性がなくなりました。(指摘部位：Management LAN Port1)
	FD78h モジュールの冗長性がなくなりました。(指摘部位 : Management LAN Port)
インフォメーション	モジュールの冗長性が回復しました。(指摘部位：Management LAN Port0)
	モジュールの冗長性が回復しました。(指摘部位：Management LAN Port1)
	モジュールの冗長性が回復しました。(指摘部位：Management LAN Port)

※上記以外の「インフォメーション」アラートが報告される場合がありますが，システム動作には影響ありません。

- HVM で運用しているお客様は，本操作を行った場合，ネットワーク接続が一時的に切断されることにより，次が通知される場合がありますが，通信の異常は自動回復されるため問題ありません。

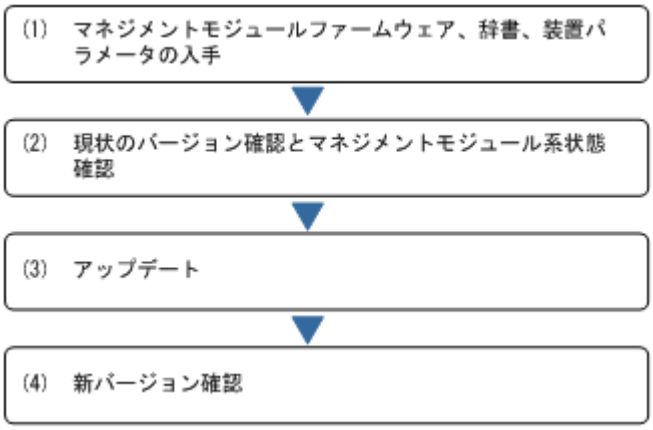
表 2-158 メッセージの通知

メッセージの通知
"SVP Access Failure"の HVM スクリーン表示
JP1/ServerConductor/BladeServerManager への次のアラート報告 「警告」アラート：0x162F 物理パーティション x で HVM とマネジメントモジュール間の通信異常が発生しました。 HCSM への次のアラート報告 「警告」アラート：FD43 h 物理パーティションで警告イベントが発生しました。(指摘部位 : Partition N - HVM，発生事象：communication error (HVM - Management Module)

- HA モニタを導入しているお客様は，バージョンアップ作業中，タイミングによって HA モニタでリセットパス異常のメッセージ（KAMN624-E，KAMN399-E）が出力される場合があり，以降の監視を中止します。バージョンアップ作業中はシステムの状態を監視できる環境で実施してください。本メッセージ出力時は，バージョンアップ以外の他要因(ハードエラー etc)でも出力される可能性があるため，必ず monrp コマンドを実行しパスが正常(status が"OK")であることの確認とリセットパスの監視再開を実施してください。(status が"OK"以外の場合は，他要因による障害が考えられ，自動フェールオーバができない可能性がありますので，保守担当者に対処を依頼してください。)
- バージョンアップ作業中は，マネジメントモジュールへのレスポンス低下の恐れがあるため，バージョンアップ作業は極力業務への影響が少ない時間帯に行ってください。
- バージョンアップ作業中にマネジメントモジュールの交替が発生すると，バージョンアップ作業は失敗します。障害要因を取り除いた後，再実行してください。
- HCSM を使用してアップデートを実行する場合，アップデート実行後に"シャーシ情報更新"を実行してから，バージョンを確認してください。
- ファームウェアのダウングレードをする際は，お買い求め先または保守員まで連絡してください。

アップデートの流れと操作方法

次にマネジメントモジュールファームウェア，辞書，装置パラメータのアップデートの流れと操作方法を示します。



アップデート後は必ずバージョンを確認し，期待するバージョンが表示されていることを確認してください。

表 2-159 Web コンソールでの操作方法

項目	画面
マネジメントモジュールファームウェア，辞書，装置パラメータのバージョン表示	Resources タブ → Modules → 全モジュール → マネジメントモジュール → マネジメントモジュール x → 状態タブ
マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート	Resources タブ → Modules → 全モジュール → マネジメントモジュール → Action → ファームウェアアップデート

表 2-160 CLI コンソールでの操作方法

項目	コマンド
マネジメントモジュールファームウェア，辞書，装置パラメータのバージョン表示	show mgmt-module firmware
マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート	update mgmt-module firmware

表 2-161 LCD タッチコンソールでの操作方法

項目	画面
マネジメントモジュールファームウェア，辞書，装置パラメータのバージョン表示	ハードウェア保守 → マネジメントモジュール(MM) → 詳細表示
マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート	ハードウェア保守 → マネジメントモジュール(MM) → ファームウェア更新

参考

- HCSM を使用してアップデートを実行する場合，マネジメントモジュールのファームウェアバージョンが A0150 以降である必要があります。
- HCSM を使用してアップデートを実行する際の操作方法および手順は，HCSM に付属のマニュアルを参照してください。

次に Web コンソールを使用した，マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート手順を説明します。

(1) マネジメントモジュールファームウェア，辞書，装置パラメータの入手

マネジメントモジュールファームウェア，辞書，装置パラメータを BladeSymphony ホームページからダウンロードしてください。

ホームページアドレス：http://www.hitachi.co.jp/products/bladesymphony/

次のとおりに進むことで，ファームウェアの掲載ページを表示することができます。

[サポート＆ダウンロード]

↓

[ドライバ・ユーティリティダウンロード]の[詳細はこちら]

↓

[ダウンロード最新情報一覧]の[ファームウェア]

ダウンロードするファイルは次の通りです。

ダウンロードしたファイルを解凍してください。

アップデート対象	ダウンロードファイル	解凍結果
マネジメントモジュールファームウェア	BS500 マネジメントモジュールファームウェア	svpfw.AXXXX-X-XXXX.update readme.txt
辞書	BS500 辞書	dict.AXXXX.update readme.txt
装置パラメータ	BS500 装置パラメータ	sdpara.XXXX.update readme.txt

XXXX はバージョンを表します。

各アップデートには xxxxx.update ファイルを使用してください。

重要

- ファイル名の変更はしないでください。ファイル名が変更された場合，マネジメントモジュールはファームウェアファームウェアファイルとして認識できません。
- 別機種(例：BS2000)のファイルは適用できません。

(2) 現状のバージョン確認とマネジメントモジュール系状態確認

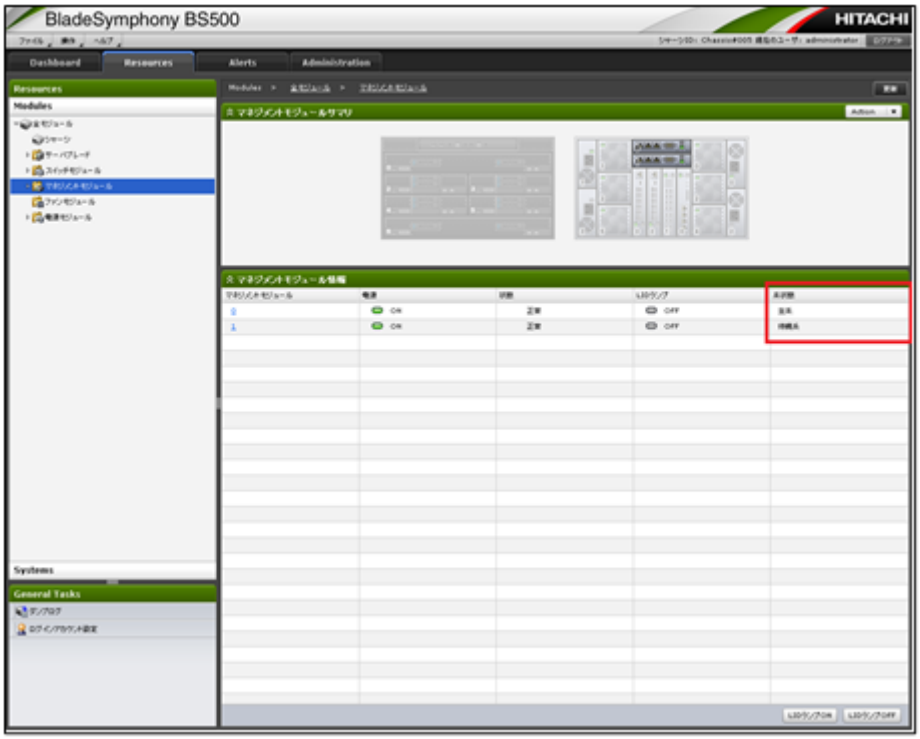
アップデートを実施する前に，「(1) マネジメントモジュールファームウェア，辞書，装置パラメータの入手」で入手したアップデート対象のマネジメントモジュールファームウェア，辞書，装置パラメータのバージョンが，現在のバージョンより新しいことを確認してください。

また，マネジメントモジュールファームウェアのアップデートを実施する場合，マネジメントモジュールのリブートで接続が切れます。アップデート後にマネジメントモジュールの系状態がアップデート前と後で同じかどうかで，マネジメントモジュールとの接続状態を確認します。そのためマネジメントモジュールの系状態の確認もしてください。

1. [Resources]タブをクリックします。
2. [Resources]パネルの[全モジュール情報]内の[モジュール種別]の「マネジメントモジュール」をクリックします。

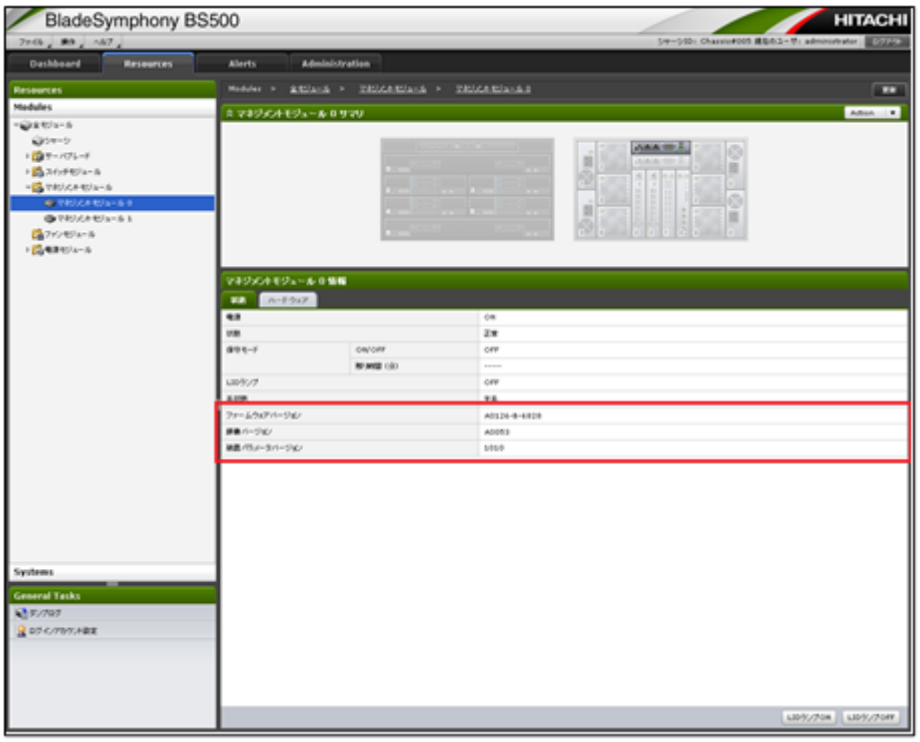
参考 手順 3 は，マネジメントモジュールファームウェアアップデートを実施する場合に，実施してください。

3. マネジメントモジュール 0，1 のそれぞれの系状態を確認してください。



参考 この確認結果をアップデート後の確認に使用します。

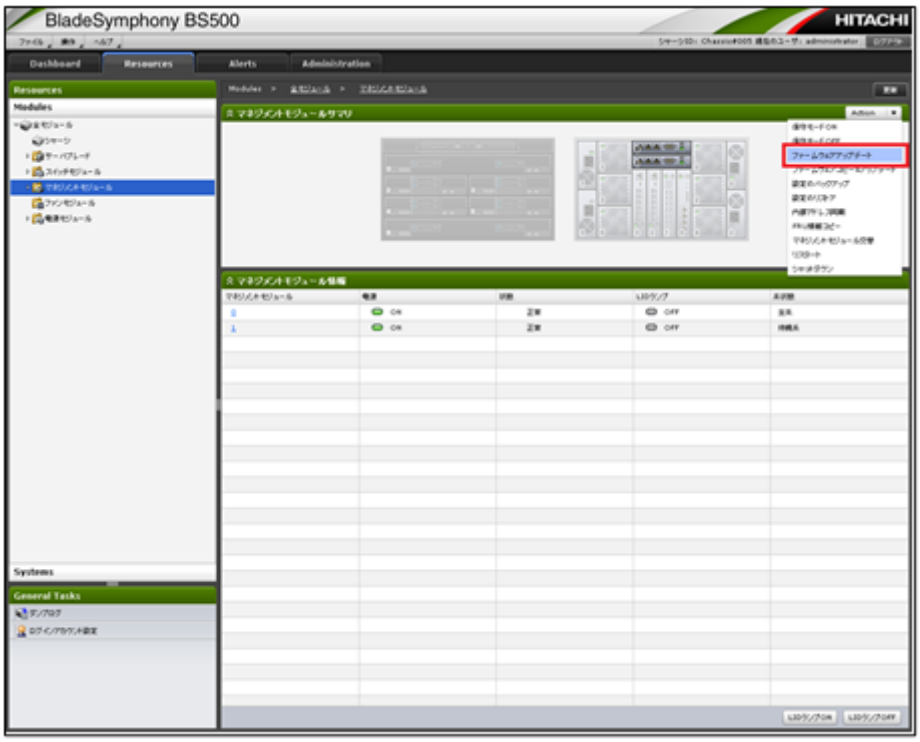
4. マネジメントモジュール情報の系状態が主系と表示されているマネジメントモジュール番号をクリックします。
5. 「ファームウェアバージョン」，「辞書バージョン」，「装置パラメータバージョン」でそれぞれの現在のバージョンを表示しています。「(1) マネジメントモジュールファームウェア，辞書，装置パラメータの入手」で入手した，アップデート対象のマネジメントモジュールファームウェア，辞書，装置パラメータバージョンの方が新しいことを確認してください。



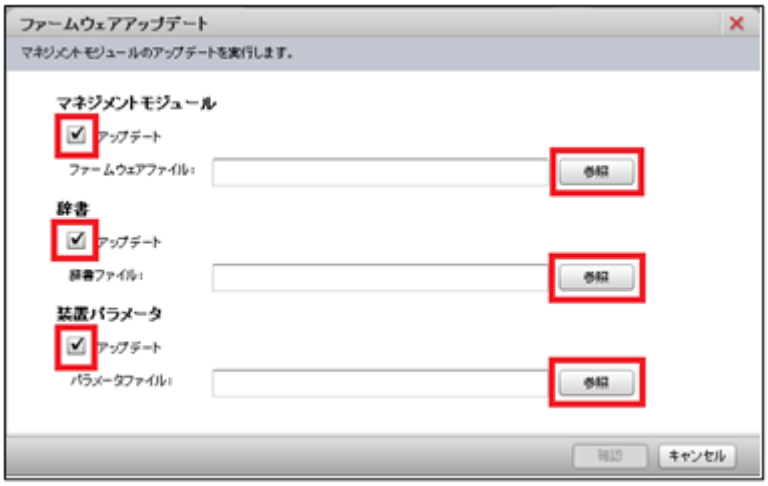
(3) アップデート

マネジメントモジュールファームウェア，辞書，装置パラメータのアップデート手順を説明します。

1. これからアップデートを実施するアップデートファイルを，システムコンソールのハードディスクなどに格納してください。複数のアップデートを実施する場合は，アップデートを実施する全ファイルを格納してください。
2. [Resources]タブをクリックします。
3. [Resources]パネルの[全モジュール情報]内の[モジュール種別]の「マネジメントモジュール」をクリックします。
4. [Action]コンボボックスで「ファームウェアアップデート」をクリックします。

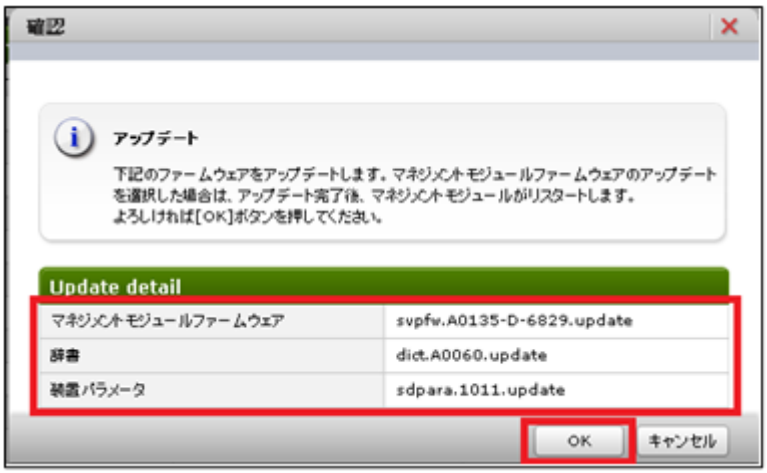


5. [ファームウェアアップデート]ダイアログで，アップデートを実施する対象のチェックボックスにチェックをつけ，[参照]ボタンをクリックし，アップデートファイルを選択します。



参考 ファイルを開く手順については，OS の操作手順に従ってください。

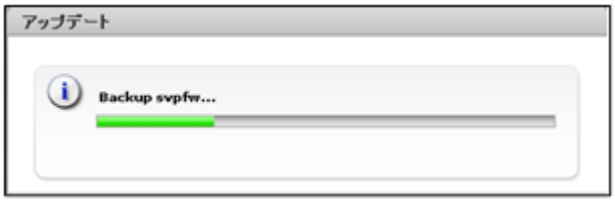
6. [ファームウェアアップデート]ダイアログで，[確認]ボタンをクリックします。
7. アップデートファイルが各アップデート対象に表示されていることを確認し，[OK]ボタンをクリックします。



8. ファームウェアのアップロードが実行し，アップロードのプログレスバーが終了次第，アップデートが続けて実行され，アップデートのプログレスバーが表示されます。アップデートのプログレスバーでは現在実行中の動作が表示されます。アップデートが終了するまで 10 数分待ってください。

   アップロードのプログレスバー

   アップデートのプログレスバー



9. アップデートのプログレスバーが終了すれば，アップデートは終了します。[閉じる]ボタンをクリックします。マネジメントモジュールファームウェアのアップデートを実施しているかどうかで表示が変わります。

   マネジメントモジュールファームウェアのアップデート実施時

参考 上記メッセージが表示される前に，アップデート完了による主系マネジメントモジュールのリブートが開始される場合があります。

この場合，Web コンソールの画面に「要求がタイムアウトになりました」というメッセージが表示されます。

このメッセージが表示された場合は，約 10 分後に「(4) 新バージョン確認」の手順に従い，バージョンを確認してください。アップデートを実施したバージョンになっていることが確認できた場合は問題ありません。確認の際に Web コンソールに接続できない場合は，お買い求め先，または保守員まで連絡してください。

マネジメントモジュールファームウェアなしのアップデート実施時

10. マネジメントモジュールファームウェアのアップデートをした場合，主系マネジメントモジュールのリブートで接続がきれるので，ブラウザを閉じてください。

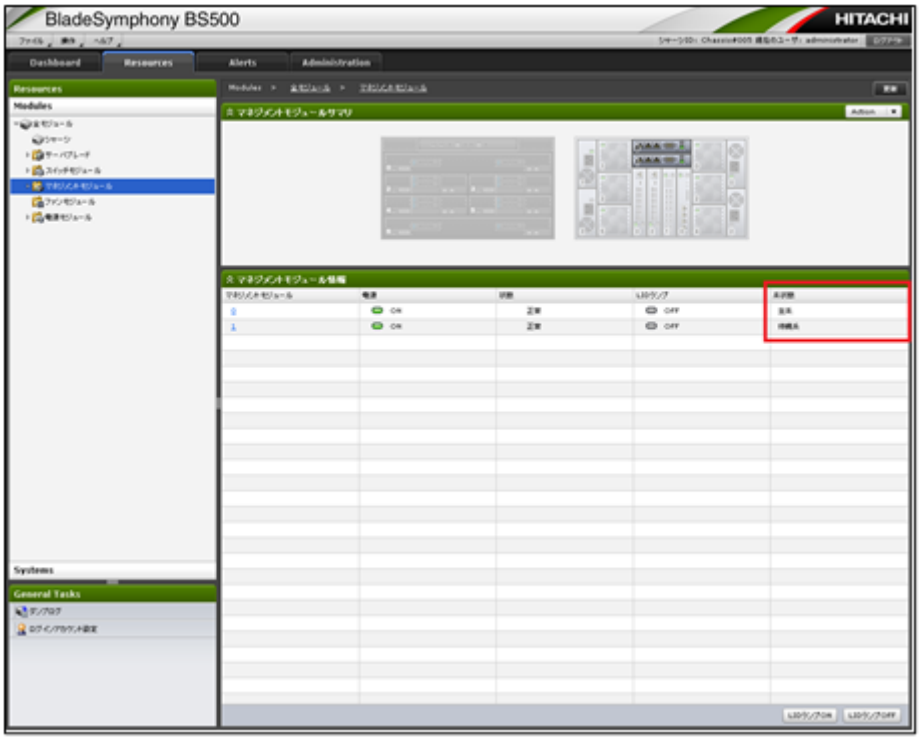
参考 マネジメントモジュールファームウェアなしのアップデート実施時にはブラウザを閉じる必要はありません。続けて「(4) 新バージョン確認」を行ってください。

(4) 新バージョン確認

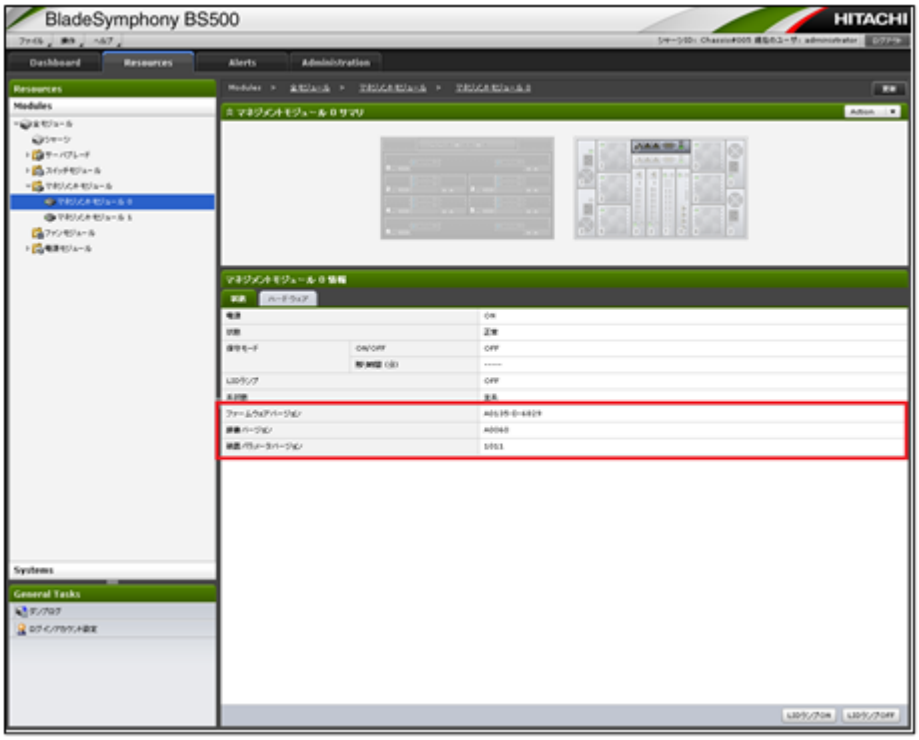
「(1) マネジメントモジュールファームウェア，辞書，装置パラメータの入手」で入手したバージョンに正しくアップデートできたかを確認します。

参考 手順 1～4 は，マネジメントモジュールファームウェアのアップデートをしたとき実施してください。
主系マネジメントモジュールのリブート後，もう 1 台のマネジメントモジュールのリブートが実施されます。もう 1 台のマネジメントモジュールのリブートが終了する約 10 分後に再度ブラウザを開き，ログインを実施してください。
マネジメントモジュールリブート中ではログインできないので，その際は数分待った後に再度実施してください。

1. ブラウザを開き，ログインします。
   [User ID]と[Password]を入力して，[Log In]ボタンをクリックします。
2. [Resources]タブをクリックします。
3. [Resources]パネルの[全モジュール情報]内の[モジュール種別]の「マネジメントモジュール」をクリックします。
4. マネジメントモジュール情報の系状態が，アップデート実施前の系状態と同じ状態になっていれば，マネジメントモジュールファームウェアアップデートは完了しています。マネジメントモジュール 0，1 の系状態を確認してください。



5. アップデート実施したバージョンが表示されることを確認します。マネジメントモジュール情報の系状態が主系と表示されているマネジメントモジュールをクリックします。
6. 「ファームウェアバージョン」,「辞書バージョン」,「装置パラメータバージョン」でそれぞれの現在のバージョンを表示しています。アップデートを実施したバージョンが表示されていることを確認してください。



2.29.3 サーバブレードファームウェアのアップデート

サーバブレードファームウェアのアップデートは，マネジメントモジュールのコンソールまたはHCSM(Ver7.5 以降)から実施できます。

サーバブレードファームウェアは BMC と UEFI を含んでおり，サーバブレードファームウェアをアップデートすると，BMC と UEFI が両方同時にアップデートされます。

同一サーバシャーシ内に搭載された同一種類のサーバブレードを複数台同時にサーバブレードのファームウェアのアップデートを実施することも可能です。

表 2-162 複数台同時アップデートの実施可否

Web コンソール	CLI コンソール	LCD タッチコンソール
○	○	×

サーバブレードのファームウェアのアップデートは，マネジメントモジュールのコンソールからアップデート実施後に，バックグラウンドでアップデート処理が実施されます。

マネジメントモジュールのコンソールでの操作は約 5～10 分で終了し，その後バックグラウンドでアップデート処理が約 10～30 分実施されます。

サーバブレードファームウェアアップデート時の制限事項

サーバブレードファームウェアのアップデートを行う場合，次の制限事項があります。

- サーバブレードのアップデートを実行する際は，サーバブレードの電源を OFF してから実行してください。

- 複数種類のサーバブレードのファームウェアのアップデートには対応しておりません。サーバブレードのファームウェアのアップデートは 1 回につき，1 種類のサーバブレードのみ実施可能です。

参考

- 例えば，BS520H サーバブレード A1/B1/A2/B2/B3 を複数台同時にファームウェアのアップデートを実施することは対応しておりますが，BS520H サーバブレード A1/B1/A2/B2/B3 と BS520A サーバブレード A1 を同時にアップデートすることには対応しておりません。
- サーバブレードの種類は，Web コンソールのサーバブレードのハードウェアタブの[名称]で確認することができます。詳細は「*BladeSymphony BS500 Web コンソール ユーザーズガイド*」を参照してください。
- 複数種類のサーバブレードのアップデートを実施したい場合は，アップデート完了確認後に実施してください。

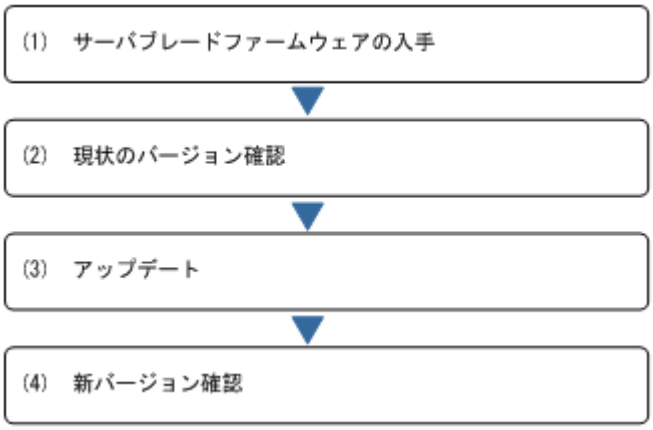
- サーバブレードのファームウェアのアップデート作業中，BMC が再起動を実施するため，マネジメントモジュールとの通信ができなくなる場合があります。その際に，次の警告 SEL が採取されますが，問題はありません。

  サーバブレード SVP-BMC 間通信障害発生(IPMI over LAN)
- サーバブレードのファームウェアのアップデート作業中は，サーバブレードの抜去や操作は実施しないでください。
- サーバブレードの稼働中にアップデートを実施した場合，サーバブレードファームウェア内の UEFI のアップデートは，次回のサーバブレード電源 ON 時に反映されます。その際，通常よりも電源 ON の時間がかかります。
- アップデート処理中にサーバブレードの電源を ON した場合，アップデート処理が完了した後に電源 ON します。
- バックグラウンドでの処理後の最初の Post 中に電源 OFF しないでください。実施した場合，タイミングによってはサーバブレードが正常に起動しなくなる場合があります。
- マネジメントモジュールのコンソールからのアップデート実施中に，マネジメントモジュールの交替が発生した場合，アップデートが失敗します。障害要因を取り除いた後，再実行してください。

アップデートの流れと操作方法

次にサーバブレードファームウェアのアップデートの流れと操作方法を示します。

図 2-11 アップデートの流れ



アップデート後は必ずバージョンを確認し，期待するバージョンが表示されていることを確認してください。

表 2-163 Web コンソールでの操作方法

項目	画面
サーバブレードファームウェアのバージョン表示	Resources タブ → Systems → ファームウェア管理 → サーバブレードタブ
サーバブレードファームウェアのアップデート	Resources タブ → Systems → ファームウェア管理 → サーバブレードタブ → サーバブレードファームウェアアップデート

表 2-164 CLI コンソールでの操作方法

項目	コマンド
サーバブレードファームウェアのバージョン表示	show blade firmware
サーバブレードファームウェアのアップデート	update blade firmware

表 2-165 LCD タッチコンソールでの操作方法

項目	画面
サーバブレードファームウェアのバージョン表示	ハードウェア保守 → サーバブレード(SB) → 詳細表示
サーバブレードファームウェアのアップデート	ハードウェア保守 → サーバブレード(SB) → ファームウェア更新

参考

- HCSM を使用してアップデートを実行する場合，マネジメントモジュールのファームウェアバージョンが A0150 以降である必要があります。
- HCSM を使用してアップデートを実行する際の操作方法および手順は，HCSM に付属のマニュアルを参照してください。

次に Web コンソールを使用した，サーバブレードファームウェアのアップデート手順を説明します。

(1) サーバブレードファームウェアの入手

サーバブレードファームウェアを BladeSymphony ホームページからダウンロードしてください。

ホームページアドレス：http://www.hitachi.co.jp/products/bladesymphony/

次のとおりに進むことで，ファームウェアの掲載ページを表示することができます。

[サポート&ダウンロード]

↓

[ドライバ・ユーティリティ ダウンロード]の[詳細はこちら]

↓

[ダウンロード最新情報一覧]の[ファームウェア]

ダウンロードするファイルは次の通りです。

ダウンロードしたファイルを解凍してください。

モデル名	ダウンロードファイル		解凍結果
BS520H サーバブレード A1/B1/A2/B2/B3	BS500 サーバブレードファームウェア	BS520H サーバブレード	520h_x1_XXXX.update readme.txt

モデル名	ダウンロードファイル		解凍結果
BS520A サーバブレード A1		BS520A サーバブレード	520a_x1_XXXX.update readme.txt
BS540A サーバブレード A1/B1		BS540A サーバブレード	540a_x1_XXXX.update readme.txt

XXXX はバージョンを表します。各アップデートには xxxxx.update ファイルを使用してください。

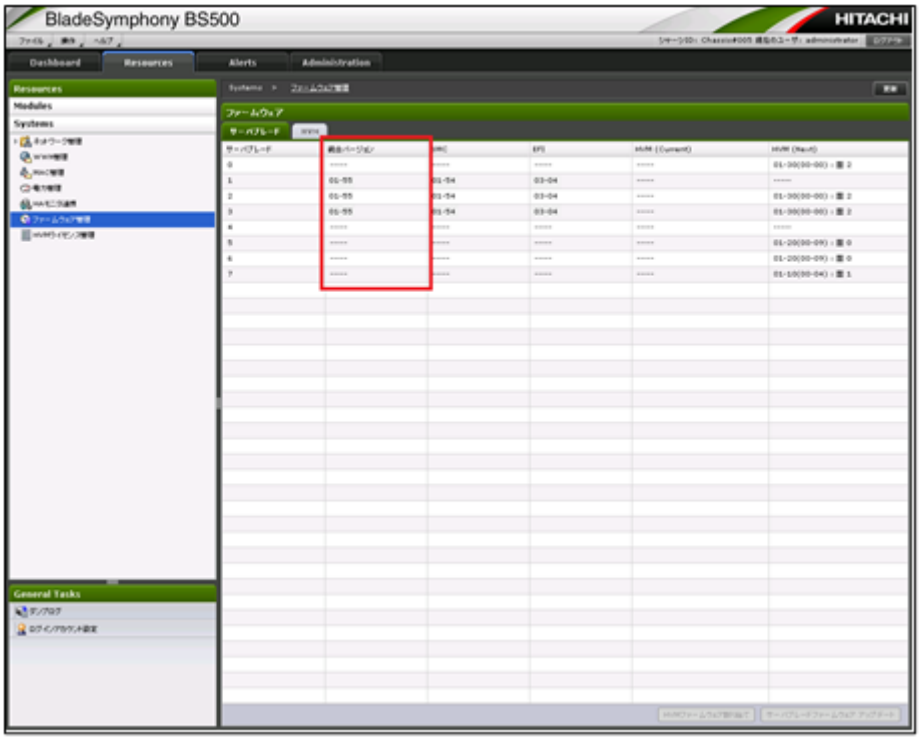
参考

- 別モデルのファームウェアを使用してファームウェアのアップデートを行うと，アップデートが失敗します。この場合，適切なファイルを使用して，再度アップデート操作を実行してください。
- ファイル名の変更は行わないでください。ファイル名が変更されると，マネジメントモジュールはファームウェアファイルと認識することができません。
- 他機種(例：BS2000)のファイルは適用できません。

(2) 現状のバージョン確認

アップデートを実施する前に，「(1) サーバブレードファームウェアの入手」で入手したアップデート対象のサーバブレードファームウェアのバージョンが，現在のバージョンより新しいことを確認してください。

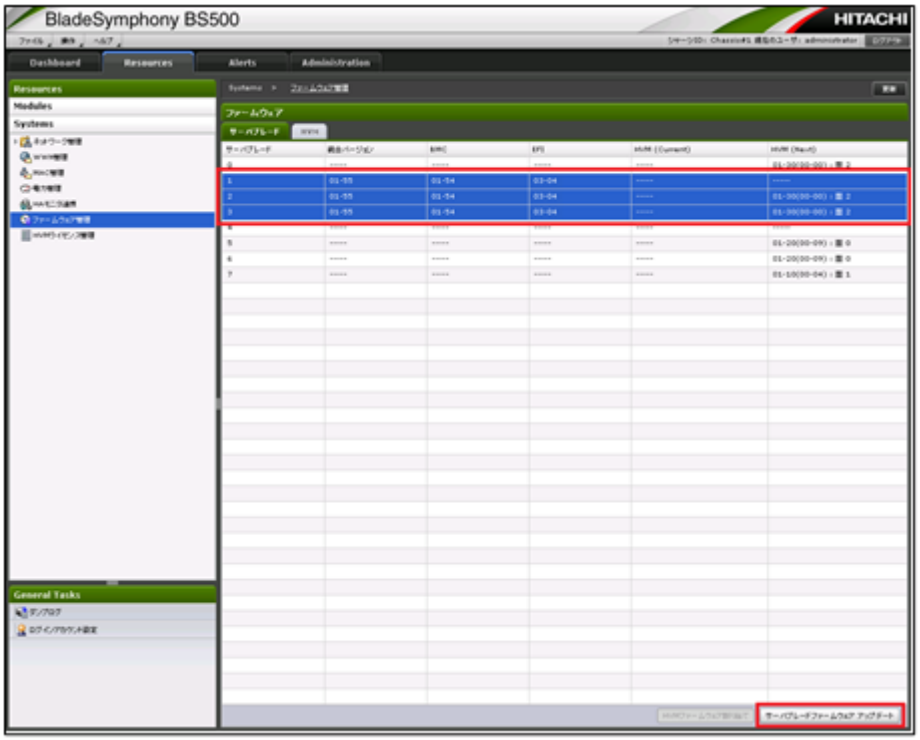
1. [Resources]タブをクリックします。
2. [Resources]パネルの[Systems]内の[ファームウェア管理]をクリックします。
3. [サーバブレード]タブの[統合バージョン]で，現在のバージョンを表示しています。アップデート対象となる全てのサーバブレードで，アップデート対象のサーバブレードファームウェアのバージョンの方が新しいことを確認してください。



(3) アップデート

サーバブレードのファームウェアのアップデートは，マネジメントモジュールのコンソールからアップデート実施後に，バックグラウンドでアップデート処理が実施されます。

1. アップデートを実施するアップデートファイルを, システムコンソールのハードディスクなどに格納してください。
2. [Resources]タブをクリックします。
3. [Resources]パネルの[Systems]内の[ファームウェア管理]をクリックします。
4. アップデート対象のサーバブレードをクリックし, 選択します。サーバブレードが選択された状態で[サーバブレードファームウェアアップデート]をクリックします。



参考

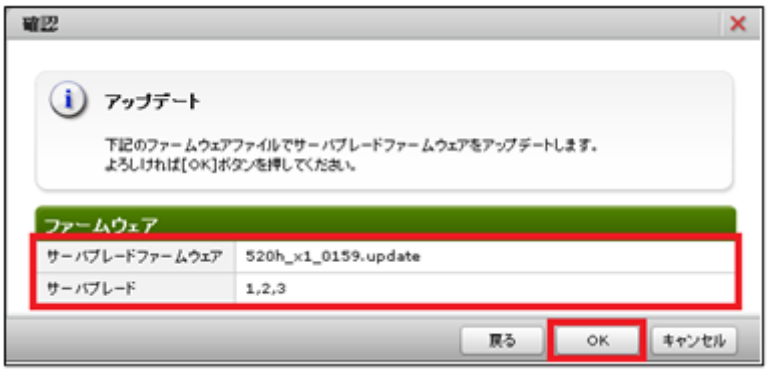
- 複数台のサーバブレードを選択する場合は，[Ctrl]キーを押しながら，サーバブレードをクリックしてください。
- 選択されると行が青くなります。
- SMP 構成の場合，プライマリサーバブレードを選択すると，SMP を構成するすべてのサーバブレードのファームウェアがアップデートされます。
- ノンプライマリブレードは，SMP 構成時にファームウェアアップデートをしてから SMP 構成を解除した場合，最初の起動時に時間がかかります。

5. [サーバブレードファームウェアアップデート]ダイアログの[参照]ボタンをクリックし，アップデートファイルを選択します。

参考 ファイルを開く手順については，OS の操作手順に従ってください。

6. [サーバブレードファームウェアアップデート]ダイアログの[確認]ボタンをクリックします。

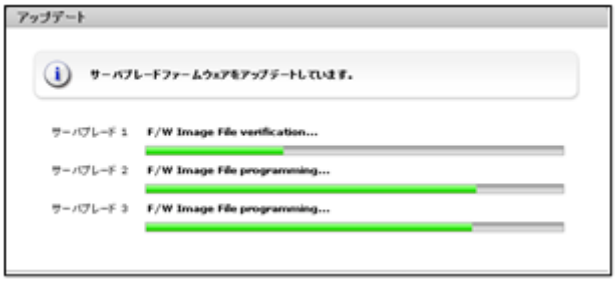
7. 選択したアップデートファイルが[サーバブレードファームウェア]に表示されていることと，対象となる全サーバブレードが[サーバブレード]に表示されていることを確認し，[OK]ボタンをクリックします。



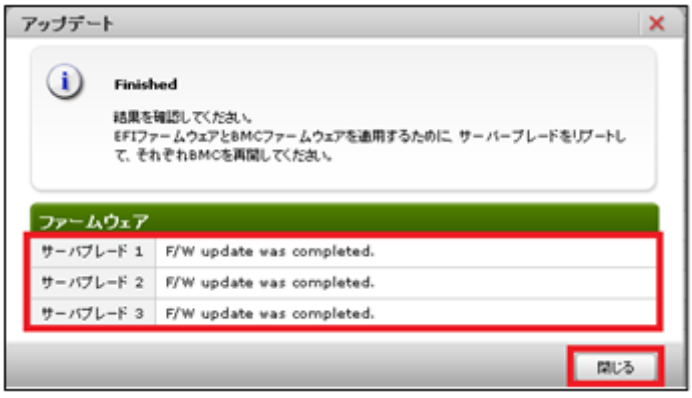
8. ファームウェアのアップロードが実行し，アップロードのプログレスバーが終了次第，アップデートが続けて実行され，アップデートのプログレスバーが表示されます。アップデートのプログレスバーでは現在実行中の動作が対象となる全サーバブレードで表示されます。アップデートが終了するまで数分待ってください。

アップロードのプログレスバー

アップデートのプログレスバー



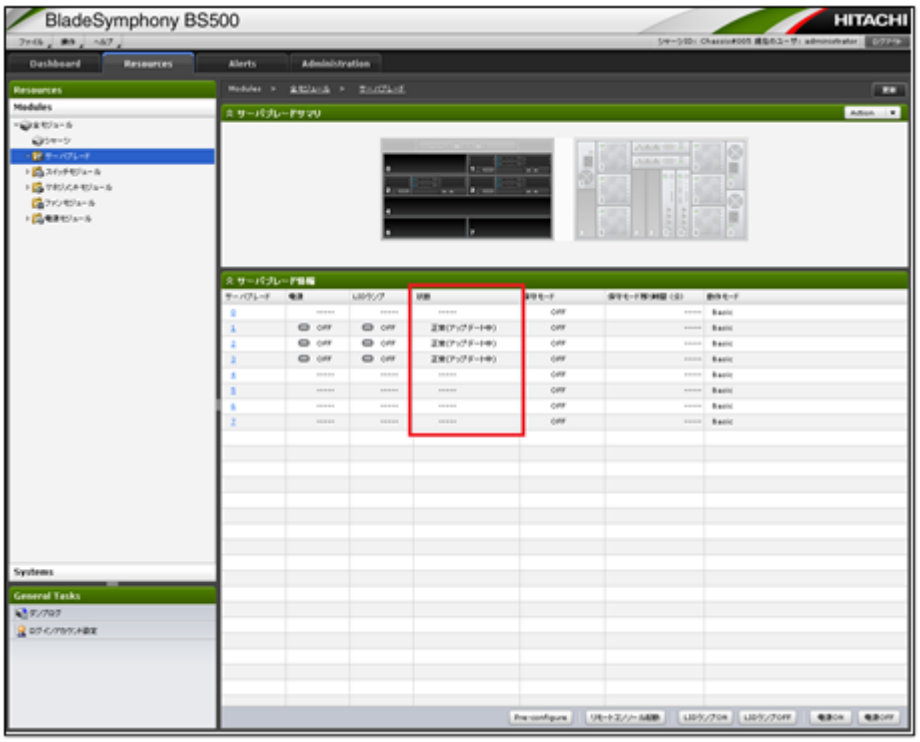
9. 対象となる全サーバブレードのアップデート結果が表示されるので，成功していることを確認し，[閉じる]ボタンをクリックします。



10. バックグランドでのアップデート処理が実施されるので，その処理経過を確認します。[Resources]パネルの[Modules]内の[全モジュール]をクリックします。

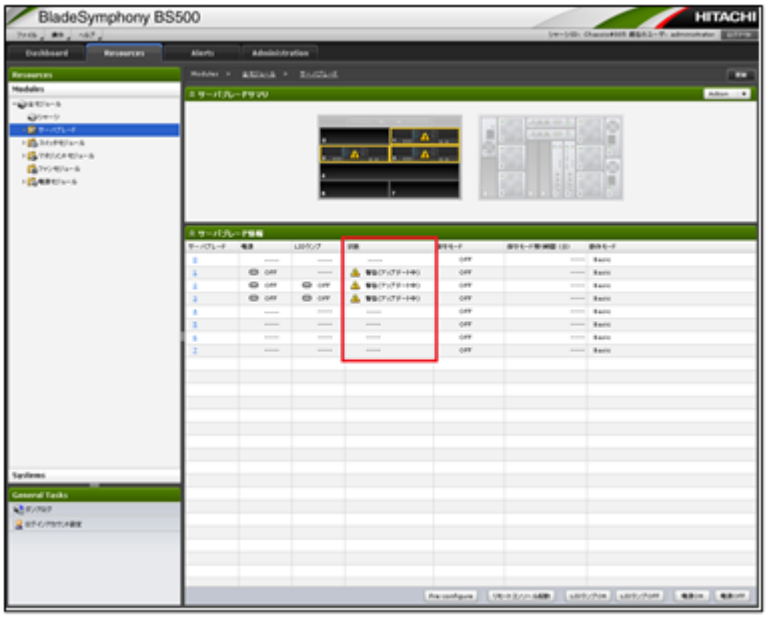
11. [全モジュール情報]内の[モジュール種別]の「サーバブレード」をクリックします。

12. 対象となる全サーバブレードの[サーバブレード情報]の[状態]の表示が，[正常(アップデート中)]から[正常]になるまで，約 10～30 分待ってください。

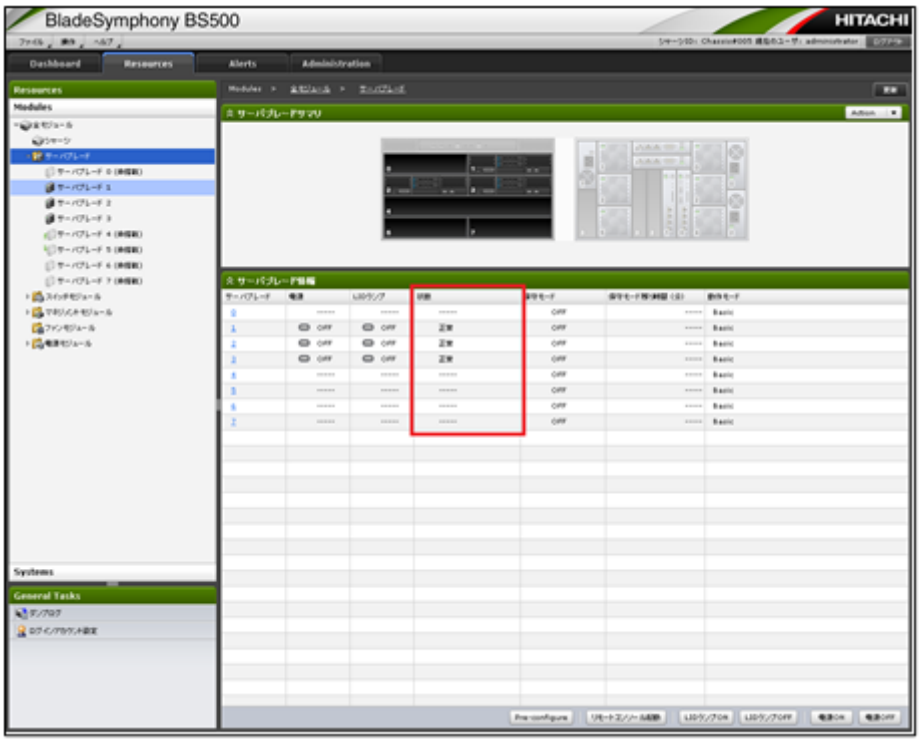


参考

- [状態]タブの表示は自動更新されないため，画面右上の[更新]ボタンをクリックし，定期的に表示を更新してください。
- 「サーバブレードファームウェアアップデート時の制限事項」より，「サーバブレード SVP-BMC 間通信障害発生(IPMI over LAN)」SEL が採取されることがありますが，採取された場合，[サーバブレード情報]の[状態]の表示が「警告(アップデート中)」になることがあります。この場合でも，表示が[正常]となれば，アップデートは終了します。



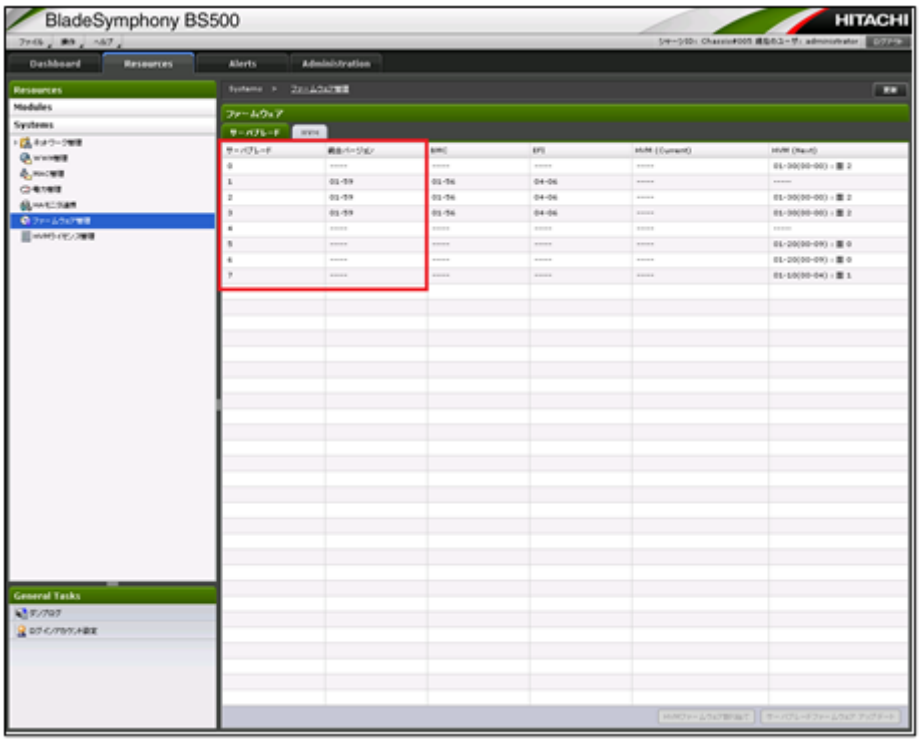
13. 表示が[正常]となれば，アップデートは終了します。



(4) 新バージョン確認

「(1) サーバブレードファームウェアの入手」で入手したバージョンに正しくアップデートできたかを確認します。

1. [Resources]パネルの[Systems]内の[ファームウェア管理]をクリックします。
2. [サーバブレード]タブの[統合バージョン]で，現在のバージョンを表示しています。アップデートを実施した全てのサーバブレードで，アップデート対象のサーバブレードファームウェアのバージョンが表示されることを確認してください。



2.30 設定の保存と復元

マネジメントモジュールで実施する，設定の保存と復元について説明します。

2.30.1 マネジメントモジュールから保存，復元可能な設定

マネジメントモジュールからは，次の設定の保存と復元が実施可能です。

表 2-166 保存と復元

項目	マネジメントモジュールから可能な操作
マネジメントモジュール設定	保存と復元
ファイバチャネル拡張カード設定	保存
HVM 設定	保存と復元

2.30.2 マネジメントモジュール設定

マネジメントモジュールの設定の保存と復元について説明します。

(1) 保存

マネジメントモジュール設定の保存は，マネジメントモジュールのコンソールから実施することができます。マネジメントモジュール設定の保存には数分かかります。

重要

- マネジメントモジュールを非冗長構成で使用されている場合は，必ずマネジメントモジュール設定の保存を実施し，大切に保管してください。マネジメントモジュールが故障した場合に，設定を保存したファイルがないと，設定を元に戻すことができません。
- 設定の保存の実行中に，コンソールからの設定の変更や，サーバブレードの電源状態が変化すると，設定の保存は失敗することがあります。これらが発生しない状態で設定の保存を実施してください。

表 2-167 Web コンソールでの操作方法

項目	画面
マネジメントモジュール設定の保存	Resources タブ → Modules → 全モジュール → マネジメントモジュール(アクションメニュー) → 設定のバックアップ

(2) 復元

マネジメントモジュール設定の復元は，マネジメントモジュールのコンソールから実施することができます。マネジメントモジュール設定の復元には数分かかり，復元が完了するとマネジメントモジュールがリブートします。

重要 マネジメントモジュール設定を復元するとマネジメントモジュールがリブートするため，マネジメントモジュールの動作が停止します。サーバブレードの稼働中にマネジメントモジュール設定の復元は実施しないでください。

参考

- マネジメントモジュール設定を復元すると，HVM 設定も，マネジメントモジュール設定を保存した時と同じ設定に復元されます。
- バックアップファイルを採取したマネジメントモジュールファームウェアバージョンより，新しいバージョンのマネジメントモジュールにマネジメントモジュール設定を復元する際，バックアップファイル採取時にサポートされていなかった機能の設定は，すべてデフォルト値で設定されます。

表 2-168 Web コンソールでの操作方法

項目	画面
マネジメントモジュール設定の復元	Resources タブ → Modules → 全モジュール → マネジメントモジュール(アクションメニュー)

2.30.3 Hitachi ファイバチャネル拡張カード設定

Hitachi ファイバチャネル拡張カードの設定の保存について説明します。

(1) 保存

Hitachi ファイバチャネル拡張カード設定の保存は，マネジメントモジュールのコンソールから実施することができます。

マネジメントモジュールには，最新 5 世代分の Hitachi ファイバチャネル拡張カード設定が，拡張カードごとに保存されます。マネジメントモジュールのコンソールから，Hitachi ファイバチャネル拡張カード設定の保存を実行するとき，マネジメントモジュールに保存されている各拡張カードの 5 世代の設定情報から，どの設定情報を保存するかを選択して，外部記憶装置に保存できます。

Hitachi ファイバチャネル拡張カード設定の保存には，数分かかります。

重要 Hitachi ファイバチャネル拡張カード GG-CC3M8G2N1(EX)/GG-CC3M8G2N2(EX)/GG-CC3M162N1(EX)/GG-CC3M162N2(EX)のみの機能です。GG-CC3M8G1N1(EX) /GG-CC3M161N1(EX)では実行できません。

表 2-169 CLI コンソールでの操作方法

項目	コマンド
Hitachi ファイバチャネル拡張カード設定の保存	backup blade fc-hba

2.30.4 HVM 設定

HVM 設定の保存と復元について説明します。

(1) 保存

ここでは，「HVM 設定のバックアップ」のことを，「HVM 設定の保存」と呼びます。

HVM 設定の保存は，マネジメントモジュールのコンソールから実施することができます。HVM 設定の保存には数分かかります。

参考 本操作では，マネジメントモジュールに保存された HVM 設定ファイルを，管理サーバなどのシステム装置の外部に出力します。システム装置内で，マネジメントモジュールに現在の HVM 設定を保存するには，「2.19 HVM 連携」を参照してください。

表 2-170 Web コンソールでの操作方法

項目	画面
HVM 設定の保存	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x(アクションメニュー)

(2) 復元

ここでは，「HVM 設定のリストア」のことを，「HVM 設定の復元」と呼びます。

HVM 設定の復元は，マネジメントモジュールのコンソールから実施することができます。HVM 設定の保存には数分かかります。

HVM 設定の復元を行う場合，次の要件を満たしたバックアップファイルを適用してください。

（1）同一 HVM のバックアップファイルであること

（2）現在の HVM ファームウェアバージョンが割り当てられている際にバックアップしたファイルであること

これらの要件を満たしていないファイルを用いた場合，HVM が起動しない，または HVM が正常に動作しないことがあります。

重要 HVM 設定の復元は，サーバブレードが電源 OFF の間のみ実施することができます。

表 2-171 Web コンソールでの操作方法

項目	画面
HVM 設定の復元	Resources タブ → Modules → 全モジュール → サーバブレード → サーバブレード x(アクションメニュー)

3

ソフトウェアのライセンス情報

この章では，ソフトウェアのライセンス情報について説明します。

❒ 3.1 ソフトウェアのライセンス情報

3.1 ソフトウェアのライセンス情報

マネジメントモジュールのファームウェアでは，弊社が開発または作成したソフトウェアの他に，次に記述するオープンソースソフトウェアをそれぞれのソフトウェアのソフトウェア使用許諾契約書に従い使用しています。該当するソフトウェア，および同ソフトウェアの使用許諾契約書の詳細につきましては，次の表を参照してください。

弊社は，お客様の要求に応じて，GNU General Public License(GPL)など，ソースコードの提供義務が記載された使用許諾条件に基づき使用許諾されるソフトウェアのソースコードを記録媒体(CD-ROM 又は DVD)でお客様に提供いたします。その際，当社は記録媒体の費用，送料および手数料をお客様に請求いたしますのでご了承ください。なお，ソースコードの要求はマネジメントモジュールファームウェアのバージョン(マネジメントモジュールのコンソールにて確認できます)を申し添えのうえ，弊社担当営業までご連絡ください。

また，次に記述するオープンソースソフトウェアに関するお問い合わせについては，弊社担当営業にお問い合わせください。

表 3-1 オープンソースソフトウェア

ソフトウェア名	ソフトウェア使用許諾契約書
Linux Kernel libgcc	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
glibc	GNU Lesser General Public License version2.1 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/lgpl-2.1.html
libstdc++ pam	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
tcp_wrappers	TCP wrapper license ライセンスの詳細は次の URL を参照してください。 ftp://ftp.porcupine.org/pub/security/tcp_wrappers_license/
zlib	zlib License ライセンスの詳細は次のホームページをご覧ください。 http://zlib.net/zlib_license.html
SysVinit bash busybox coreutils	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
e2fsprogs gdb initscripts lftp module-init-tools	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
setup	Public Domain
vsftpd	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
openssl	OpenSSL License SSLeay license ライセンスの詳細は次の URL を参照してください。 http://www.openssl.org/source/license.html

ソフトウェア名	ソフトウェア使用許諾契約書
openssh	Berkeley Software Distribution License like ライセンスの詳細は次のホームページをご覧ください。 http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD
tcpdump	The BSD 3-Clause License License: BSD Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
ethtool	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
nkf	zlib License ライセンスの詳細は次のホームページをご覧ください。 http://zlib.net/zlib_license.html
liblconv	GNU Lesser General Public License version2.1 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/lgpl-2.1.html
U-Boot	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
net-SNMP	Berkeley Software Distribution License like ライセンスの詳細は次のホームページをご覧ください。 http://www.net-snmp.org/about/license.html
DHCP Server	ISC License ライセンスの詳細は次のホームページをご覧ください。 http://www.isc.org/software/license
ntpd	NTP License ライセンスの詳細は次のホームページをご覧ください。 http://www.opensource.org/licenses/ntp-license
telnet vconfig	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
Xinetd	オリジナルライセンス ライセンスの詳細については次の URL を参照してください。 http://www.xinetd.org/cgi-bin/cvsweb.cgi/xinetd/COPYRIGHT?rev=1.1.1.1&content-type=text/xcvsweb-markup
login util-linux	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
netkit-telnet	Copyright (c) 1988, 1990 Regents of the University of California. All rights reserved.

ソフトウェア名	ソフトウェア使用許諾契約書
	Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
iputils tslib	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
Qt/Embedded	GNU Lesser General Public License version2.1 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/lgpl-2.1.html
minicom S1D13U11 Linux 2.6.35 Framebuffer and Touchscreen driver	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
libgpg-error	GNU General Public License version2 GNU Lesser General Public License version2.1 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html http://www.gnu.org/licenses/lgpl-2.1.html
libestr libee	GNU Lesser General Public License version2.1 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/lgpl-2.1.html
rsyslogd	GNU General Public License version3 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-3.0.html
dhclient	ISC License ライセンスの詳細は次のホームページをご覧ください。 http://www.isc.org/software/license
xmlrpc-c	XML-RPC For C/C++ License Copyright (C) 2001 by First Peer, Inc. All rights reserved.

ソフトウェア名	ソフトウェア使用許諾契約書
	Copyright (C) 2001 by Eric Kidd. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Expat License Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
xmlrpc-c	Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. ABYSS Web Server License Copyright (C) 2000 by Moez Mahfoudh <mmoez@bigfoot.com>. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND

ソフトウェア名	ソフトウェア使用許諾契約書
	FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
xmlrpc-c	Python 1.5.2 License Copyright 1991, 1992, 1993, 1994 by Stichting Mathematisch Centrum, Amsterdam, The Netherlands. All Rights Reserved Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of Stichting Mathematisch Centrum or CWI or Corporation for National Research Initiatives or CNRI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. While CWI is the initial source for this software, a modified version is made available by the Corporation for National Research Initiatives (CNRI) at the Internet address ftp://ftp.python.org. STICHTING MATHEMATISCH CENTRUM AND CNRI DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM OR CNRI BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
libxml2	MIT ライセンス ライセンスの詳細は次のホームページをご覧ください。 http://www.opensource.org/licenses/mit-license.html
net-tools	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
dosfsutils	GNU General Public License version3 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-3.0.html
tar	GNU General Public License version3 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-3.0.html
cron	ISC License ライセンスの詳細は次のホームページをご覧ください。 http://www.isc.org/software/license
logrotate	GNU General Public License version2 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html
procps	GNU General Public License version2
pam-ldap	ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html

ソフトウェア名	ソフトウェア使用許諾契約書
libselinux	Public Domain
libtermcap	GNU General Public License version2 GNU Lesser General Public License version2.1 ライセンスの詳細は次のホームページをご覧ください。 http://www.gnu.org/licenses/gpl-2.0.html http://www.gnu.org/licenses/lgpl-2.1.html
portmap	Copyright (c) 1990 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
OpenLDAP	The OpenLDAP Public License ライセンスの詳細は次のホームページをご覧ください。 http://www.openldap.org/software/release/license.html
apache	Apache License Version 2.0 ライセンスの詳細は次のホームページをご覧ください。 http://www.apache.org/licenses/

A

HCSM アラートメッセージ一覧

ここでは，HCSM アラートメッセージ一覧を示します。

❒ A.1 HCSM アラートメッセージ一覧

A.1 HCSM アラートメッセージ一覧

凡例

[ID]

メッセージの ID を示します。

[レベル]

メッセージのレベルを示します。(情報/警告/障害レベル)

[メッセージ]

メッセージを示します。メッセージ内の"X"，"Y"には文字が入ります。

メッセージ一覧

ID	レベル	メッセージ
内容		
FD00	警告	シャーシ内の温度が警告レベルになりました。 (Temp(X)，指摘部位：Y)
[意味] Y に示す部位の温度が警告レベルになったことを示します。 X は高温(Upper)か低温(Lower)の区分を示します。 [対処] 継続動作可能ですが，より高い障害のレベル(メッセージ ID：FD01)に移行する可能性があるため，装置の冷却を妨げている要因がないか確認し，下記に該当する要因があれば取り除いてください。 冷却を妨げる要因としては，空調設備の不具合，装置の FAN モジュールの不具合，装置の吸気口の埃つまりなどが考えられます。 要因を取り除いても現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FD01	障害	シャーシ内の温度が障害レベルになりました。 (温度異常発生)(Temp(X)，指摘部位：Y)
[意味] Y に示す部位の温度が障害レベルになったことを示します。 X は高温(Upper)か低温(Lower)の区分を示します。 [対処] ハードウェアの保護のため，指摘モジュールを停止する場合があります。お買い求め先か，保守員に連絡してください。また，装置の冷却を妨げている要因がないか確認し，下記に該当する要因があれば取り除いてください。 冷却を妨げる要因としては，空調設備の不具合，装置の FAN モジュールの不具合，装置の吸気口の埃つまりなどが考えられます。 要因を取り除いても現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FD02	情報	シャーシ内の温度が正常レベルに回復しました。 (Temp(X)，指摘部位：Y)
[意味] Y に示す部位の温度が正常レベルに回復したことを示します。 X は高温(Upper)か低温(Lower)の区分を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD03	警告	CPU の温度が警告レベルになりました。 (Temp(X)，指摘部位：Y)
[意味] Y に示す部位の CPU の温度が警告レベルになったことを示します。 X は高温(Upper)か低温(Lower)の区分を示します。 [対処] 継続動作可能ですが，より高い障害のレベル(メッセージ ID：FD04)に移行する可能性があるため，装置の冷却を妨げている要因がないか確認し，下記に該当する要因があれば取り除いてください。 冷却を妨げる要因としては，空調設備の不具合，装置の FAN モジュールの不具合，装置の吸気口の埃つまりなどが考えられます。 要因を取り除いても現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FD04	障害	CPU の温度が障害レベルになりました。 (温度異常発生)(Temp(X)，指摘部位：Y)
[意味] Y に示す部位の CPU の温度が障害レベルになったことを示します。 X は高温(Upper)か低温(Lower)の区分を示します。		

ID	レベル	メッセージ
内容		
[対処] ハードウェアの保護のため，指摘モジュールを停止する場合があります。お買い求め先か，保守員に連絡してください。また，装置の冷却を妨げている要因がないか確認し，下記に該当する要因があれば取り除いてください。 冷却を妨げる要因としては，空調設備の不具合，装置の FAN モジュールの不具合，装置の吸気口の埃つまりなどが考えられます。 要因を取り除いても現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FD05	情報	CPU の温度が正常レベルに回復しました。 (Temp(X)，指摘部位：Y)
[意味] Y に示す部位の CPU の温度が正常レベルに回復したことを示します。 X は高温(Upper)か低温(Lower)の区分を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD10	警告	電圧が警告レベルになりました。 (Voltage(X)，指摘部位：Y)
[意味] Y に示す部位の電圧が警告レベルになったことを示します。 X は高圧(Upper)か低圧(Lower)の区分を示します。 [対処] 継続動作可能ですが，より高い障害のレベル(メッセージ ID：FD11)に移行する可能性があります。お買い求め先か，保守員に連絡してください。		
FD11	障害	電圧が障害レベルになりました。 (電圧異常発生)(Voltage(X)，指摘部位：Y)
[意味] Y に示す部位の電圧が障害レベルになったことを示します。 X は高圧(Upper)か低圧(Lower)の区分を示します。 [対処] ハードウェア保護のため，指摘モジュールを停止する場合があります。お買い求め先か，保守員に連絡してください。		
FD12	情報	電圧が正常レベルに回復しました。 (Voltage(X)，指摘部位：Y)
[意味] Y に示す部位の電圧が正常レベルに回復したことを示します。 X は高圧(Upper)か低圧(Lower)の区分を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD30	情報	モジュールが挿入されました。 (指摘部位：X)
[意味] X に示すモジュールが挿入されたことを示します。 [対処] 特に必要ありません。		
FD31	情報	モジュールが抜去されました。 (指摘部位：X)
[意味] X に示すモジュールが抜去されたことを示します。 [対処] 特に必要ありません。		
FD38	障害	ウォッチドッグタイマのタイムアウトを検出しました。 (指摘部位：X)
[意味] X に示す部位において，ウォッチドッグタイマのタイムアウトを検出したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD40	警告	サーバで警告イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレードで警告レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD41	障害	サーバで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレードで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		

ID	レベル	メッセージ
内容		
FD42	情報	サーバが回復しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレードが正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD43	警告	物理パーティションで警告イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレードで警告レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD44	障害	物理パーティションで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレードで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD45	情報	物理パーティションが回復しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレードが正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD46	警告	電源で警告イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] 電源モジュールで警告レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD47	障害	電源で障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] 電源モジュールで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD48	情報	電源が回復しました。 (指摘部位：X，発生事象：Y)
[意味] 電源モジュールが正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD4A	障害	冷却ファンで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] ファンモジュールで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD4B	情報	冷却ファンが回復しました。 (指摘部位：X，発生事象：Y)
[意味] ファンモジュールが正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD4C	警告	スイッチで警告イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] スイッチモジュールで警告レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。		

ID	レベル	メッセージ
内容		
[対処] お買い求め先か，保守員に連絡してください。		
FD4D	障害	スイッチで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] スイッチモジュールで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD4E	情報	スイッチが回復しました。 (指摘部位：X，発生事象：Y)
[意味] スイッチモジュールが正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD50	障害	ディスクで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] HDD で障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD51	情報	ディスクが回復しました。 (指摘部位：X，発生事象：Y)
[意味] HDD が正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD52	警告	管理モジュールで警告イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] マネジメントモジュールで警告レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD53	障害	管理モジュールで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] マネジメントモジュールで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD54	情報	管理モジュールが回復しました。 (指摘部位：X，発生事象：Y)
[意味] マネジメントモジュールが正常な状態に回復したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD58	警告	その他のモジュールで警告イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレード，電源モジュール，ファンモジュール，スイッチモジュール，HDD，マネジメントモジュール以外のモジュールで警告レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD59	障害	その他のモジュールで障害が発生しました。 (指摘部位：X，発生事象：Y)
[意味] サーバブレード，電源モジュール，ファンモジュール，スイッチモジュール，HDD，マネジメントモジュール以外のモジュールで障害レベルのイベントが発生したことを示します。 X はイベント発生部位を示します。Y は発生事象を示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD60	警告	冷却ファンの回転数が異常です。

ID	レベル	メッセージ
内容		
		(指摘部位：X)
[意味] X に示すファンモジュールの回転数が異常値であることを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD61	情報	冷却ファンの回転数が回復しました。 (指摘部位：X)
[意味] X に示すファンモジュールの回転数が正常値に回復したことを示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD64	警告	シャーシの AC 入力がありません。 (指摘部位：X)
[意味] X に示す電源モジュールで，AC 電源入力が無くなったことを示します。 [対処] AC 電源が正しく供給されているかを確認し，正しく供給されていている場合はお買い求め先か，保守員に連絡してください。		
FD65	情報	シャーシの AC 入力が回復しました。 (指摘部位：X)
[意味] X に示す電源モジュールで，AC 電源入力が回復したことを示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD68	障害	CPU で訂正不能障害が発生しました。 (指摘部位：X)
[意味] X に示す部位の CPU で訂正不可能なエラーが発生したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD69	警告	CPU で訂正可能障害の発生回数が監視上限を越えました。 (指摘部位：X)
[意味] X に示す部位の CPU で訂正可能なエラーが発生し，正しく訂正できましたが，訂正可能なエラーの発生回数が上限値を超えたことを示します。 [対処] 継続動作は可能ですが，今後訂正不可能な故障に移行する可能性があります。お買い求め先か，保守員に連絡してください。		
FD6B	障害	Memory で訂正不能障害が発生しました。 (指摘部位：X)
[意味] X に示す部位のメモリで訂正不可能なエラーが発生したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD6C	警告	Memory で訂正可能障害の発生回数が監視上限を超えました。 (指摘部位：X)
[意味] X に示す部位のメモリで訂正可能なエラーが発生し，正しく訂正できましたが，訂正可能なエラーの発生回数が上限値を超えたことを示します。 [対処] 継続動作は可能ですが，今後訂正不可能な故障に移行する可能性があります。お買い求め先か，保守員に連絡してください。		
FD70	警告	CPU が縮退しました。 (指摘部位：X)
[意味] X に示す部位の CPU が縮退したことを示します。 [対処] 継続動作は可能ですが，性能が低下します。お買い求め先か，保守員に連絡してください。		
FD71	警告	Memory が縮退しました。 (指摘部位：X)
[意味] X に示す部位のメモリが縮退したことを示します。 [対処] 継続動作は可能ですが，性能が低下します。お買い求め先か，保守員に連絡してください。		
FD78	警告	モジュールの冗長性がなくなりました。 (指摘部位：X)
[意味] X に示すモジュールの冗長性がなくなったことを示します。 [対処] 継続動作は可能ですが，冗長性が失われています。お買い求め先か，保守員に連絡してください。		

ID	レベル	メッセージ
内容		
FD79	情報	モジュールの冗長性が回復しました。 (指摘部位：X)
[意味] X に示すモジュールの冗長性が回復したことを示します。 [対処] 回復を示すメッセージのため，特に必要ありません。		
FD7F	情報	イベントが記録されました。 (指摘部位：X，発生事象：Y)
[意味] X に示す部位に関して，イベントが記録されたことを示します。 Y は記録されたイベントを示します。 [対処] 特に必要ありません。		
FD85	警告	サーバの電源投入が抑止されています。 (指摘部位：X)
[意味] X に示すサーバブレードの電源投入が抑止されたことを示します。 以下の原因が考えられます。 ・　構成や設定に問題がある場合（ハードウェアの組み合わせが不正／電力が不足しているなど） ・　保守作業中の場合（保守対象のモジュール／障害モジュールに対する電源操作など） [対処] 抑止原因を解消してください。抑止原因が不明の場合は，お買い求め先か，保守員に連絡してください。		
FD90	情報	サーバの電源が投入されました。 (指摘部位：X)
[意味] X に示すサーバブレードの電源が投入されたことを示します。 [対処] 特に必要ありません。		
FD91	情報	サーバの電源が切断されました。 (指摘部位：X)
[意味] X に示すサーバブレードの電源が切断されたことを示します。 [対処] 特に必要ありません。		
FD92	情報	サーバがリセットされました。 (指摘部位：X)
[意味] X に示すサーバブレードがリセットされたことを示します。 [対処] 特に必要ありません。		
FD93	障害	サーバの電源の投入に失敗しました。 (指摘部位：X)
[意味] X に示すサーバブレードの電源投入が失敗したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FD9C	情報	スイッチの電源が投入されました。 (指摘部位：X)
[意味] X に示すスイッチモジュールの電源が投入されたことを示します。 [対処] 特に必要ありません。		
FD9D	情報	スイッチの電源が切断されました。 (指摘部位：X)
[意味] X に示すスイッチモジュールの電源が切断されたことを示します。 [対処] 特に必要ありません。		
FD9F	障害	スイッチの電源の投入に失敗しました。 (指摘部位：X)
[意味] X に示すスイッチモジュールの電源投入が失敗したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FDA8	情報	電源の電源が投入されました。 (指摘部位：X)
[意味] X に示す電源モジュールの電源が投入されたことを示します。 [対処] 特に必要ありません。		

ID	レベル	メッセージ
内容		
FDA9	情報	電源の電源が切断されました。 (指摘部位：X)
[意味] X に示す電源モジュールの電源が切断されたことを示します。 [対処] 特に必要ありません。		
FDAB	障害	電源の電源の投入に失敗しました。 (指摘部位：X)
[意味] X に示す電源モジュールの電源投入が失敗したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FDAC	警告	電源の電源の切断に失敗しました。 (指摘部位：X)
[意味] X に示す電源モジュールの電源切断が失敗したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FDAE	情報	管理モジュールの電源が投入されました。 (指摘部位：X)
[意味] X に示すマネジメントモジュールの電源が投入されたことを示します。 [対処] 特に必要ありません。		
FDAF	情報	管理モジュールの電源が切断されました。 (指摘部位：X)
[意味] X に示すマネジメントモジュールの電源が切断されたことを示します。 [対処] 特に必要ありません。		
FDBA	情報	パネルボタン押下により NMI が発行されました。 (指摘部位：X)
[意味] X に示すサーバブレードにおいて，NMI を発行したことを示します。 [対処] 特に必要ありません。		
FDBB	情報	NMI が発行されました。 (指摘部位：X)
[意味] X に示すサーバブレードにおいて，NMI を発行したことを示します。 [対処] 特に必要ありません。		
FDC0	情報	時刻が更新されました。 (対象部位：X)
[意味] X に示すモジュールの時刻を変更したことを示します。 [対処] 特に必要ありません。		
FDC8	情報	F/W 更新を開始します。 (対象部位：X)
[意味] X に示すモジュールにおいて，ファームウェアの更新を開始したことを示します。 [対処] 特に必要ありません。		
FDC9	情報	F/W 更新を終了します。 (対象部位：X)
[意味] X に示すモジュールにおいて，ファームウェアの更新を終了したことを示します。 [対処] 特に必要ありません。		
FDD0	警告	装置構成の警告を検出しました。
[意味] 装置構成に問題があること示しています。 [対処] メッセージ出力前に装置構成を変更した場合は，変更に問題が無いか確認してください。 装置構成に変更が無いまたは，装置構成の変更に問題が無く，現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FDD1	障害	装置構成違反を検出しました。
[意味] 装置構成に問題があること示しています。 [対処] メッセージ出力前に装置構成を変更した場合は，変更に問題が無いか確認してください。		

ID	レベル	メッセージ
内容		
装置構成に変更が無いまたは，装置構成の変更に問題が無く，現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FDD2	警告	装置構成違反のため装置電源投入を抑止しました。 (指摘部位：X)
[意味] 装置構成違反のため装置電源投入を抑止したことを示します。 X は投入を抑止した部位を示します。 以下の原因が考えられます。 ・　構成や設定に問題がある場合（ハードウェアの組み合わせが不正／電力が不足しているなど） ・　保守作業中の場合（保守対象のモジュール／障害モジュールに対する電源操作など） [対処] 抑止原因を解消してください。抑止原因が不明の場合は，お買い求め先か，保守員に連絡してください。		
FDD3	障害	電源容量が不足しています。
[意味] 電源容量が不足していることを示します。 [対処] 電源モジュールが正しく挿入されているかを確認してください。 お買い求め先か，保守員に連絡してください。		
FDD5	障害	冷却ファンが不足しています。
[意味] ファンモジュールの数が不足していることを示します。 [対処] ファンモジュールが正しく挿入されているかを確認してください。 お買い求め先か，保守員に連絡してください。		
FF05	情報	LAN ポート<X>の系が切り替わりました。
[意味] X に示す LAN ポートの冗長化が有効になっている場合に，経路が切り替わったことを示します。 [対処] 本メッセージのみの出力であれば冗長性が確保されているので問題ありませんが， メッセージ ID：FD78 も併せて出力されている場合は，指摘 LAN ポートの接続状態を確認し，LAN ケーブル抜けや，LAN ケーブル断線でない場合は，メッセージ ID：FD78 の対処に従ってください。		
FF06	情報	LAN ポート<X>の系が復帰しました。
[意味] メッセージ ID：FF05 で切り替わった経路が，元の状態に戻ったことを示します。 [対処] 特に必要ありません。		
FF08	警告	時刻同期が行われていません。 (指摘部位：X)
[意味] X に示す部位において，NTP サーバによる時刻同期が行われていないことを示します。 [対処] マネジメントモジュールと NTP サーバが通信可能か確認してください。また，マネジメントモジュールの NTP サーバ設定および，NTP サーバとの接続，設定を見直してください。 見直し後も現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FF09	情報	時刻同期を再開しました。 (指摘部位：X)
[意味] X に示す部位において，NTP サーバによる時刻同期が再開したことを示します。 [対処] 指摘部位の時刻を確認していただき，補正が必要であれば時刻を補正してください。		
FF0B	障害	サポートセンタ通報が失敗しました。 (通報の種類：ｘ)
[意味] x に示す通報機能に障害が発生し，サポートセンタ通報が不通となっていることを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FF0E	警告	通報が失敗しました。 (通報の種類：X)
[意味] X に示す通報が失敗したことを示します。 [対処] 通報先とマネジメントモジュールが通信可能か確認してください。また，通報の設定を見直し，問題があれば修正してください。上記で回復しない場合は，お買い求め先か，保守員に連絡してください。		
FF0F	情報	通報が再開しました。 (通報の種類：X)
[意味] X に示す通報が再開したことを示します。		

ID	レベル	メッセージ
内容		
[対処] 特に必要ありません。		
FF10	情報	省電力イベントが発生しました。 (指摘部位：X，発生事象：Y)
[意味] X に示す部位において，省電力機能に関するイベントを記録したことを示します。 Y はイベントの内容を示します。 [対処] 特に必要ありません。		
FF11	警告	省電力イベント<警告>が発生しました。 (指摘部位：X，発生事象：Y)
[意味] X に示す部位において，省電力機能に関する警告レベルのイベントを記録したことを示します。 Y はイベントの内容を示します。 [対処] 必要に応じて，電力制御設定を見直してください。 電力制御設定に問題がなく，現象が回復しない場合は，お買い求め先か，保守員に連絡してください。		
FF18	情報	<X>の保守モードを開始します。
[意味] X に示す部位で，保守作業を開始したことを示します。 なお，保守作業の都合上，本メッセージが複数回出力される場合もあります。 [対処] 当該部位において保守作業を行っています。当該部位の操作を行わないようにしてください。		
FF19	情報	<X>の保守モードを終了します。
[意味] X に示す部位で，保守作業が終了したことを示します。 なお，保守作業の都合上，本メッセージが複数回出力される場合もあります。 [対処] 特に必要ありません。		
FF22	障害	<X>で Pre-configure 中に<Y>で障害を検出しました。
[意味] X に示すサーバブレードで Pre-configure 中に，Y で示す部位で障害が発生したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FF23	警告	<X>で Pre-configure 中に<Y>で不正な設定を検出しました。
[意味] X に示すサーバブレードで，Y で示す部位の設定が不正のため Pre-configure が失敗したことを示します。 [対処] Y には HBA スロット番号，ポート番号が表示されます。指摘されたスロットの HBA BIOS の 設定を見直し，修正してください。その後，Pre-configure を人手実行してください。 修正後も同じメッセージが出力される場合は，お買い求め先か，保守員に連絡してください。		
FF24	障害	<X>で Pre-configure の異常が検出されました。
[意味] X に示すサーバブレードで，Pre-configure の異常が検出されたことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FF25	警告	<X>で Pre-configure 実行中にエラーが発生しました。
[意味] X に示すサーバブレードにおいて，Pre-configure 実行中にエラーが発生したことを示します。 [対処] お買い求め先か，保守員に連絡してください。		
FF28	情報	<X>でユーザ要求による疑似障害(即時切替対象障害)が発生しました。
[意味] X に示すサーバブレードにおいて，N+M コールドスタンバイのテスト（即時切り替え）を実施したことを示します。 [対処] テストのため特に必要ありません。		
FF29	情報	<X>でユーザ要求による疑似障害が発生しました。
[意味] X に示すサーバブレードにおいて，N+M コールドスタンバイのテスト（即時切り替え以外）を実施したことを示します。 [対処] テストのため特に必要ありません。		
FF2A	障害	<X>で即時に予備機への切替が必要なイベントが発生しました。
[意味] X に示すサーバブレードにおいて，N+M コールドスタンバイによる即時切り替え対象の障害が発生したことを示します。 指摘されたサーバブレードが予備系のサーバブレードに切り替わります。		

ID	レベル	メッセージ
内容		
[対処] お買い求め先か，保守員に連絡してください。		
FF2B	障害	<X>で予備機への切替が必要なイベントが発生しました。
[意味]X に示すサーバブレードにおいて，N+M コールドスタンバイによる切り替え対象の障害が発生したことを示します。 指摘されたサーバブレードが予備系のサーバブレードに切り替わります。 [対処]お買い求め先か，保守員に連絡してください。		
FF40	警告	LPAR 割り当て済み NIC のスケジューリングモードが変更されました。(指摘部位：<X>,発生事象：<Y>)
[意味] LPAR 割り当て済み NIC のスケジューリングモードが変更されたことを示します。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] セーフモードへ移行していますので，LPAR への NIC の割り当てを確認し，必要に応じて LPAR への割り当て設定を変更の上，セーフモードを解除してください。		
FF41	障害	指定管理 NIC で障害イベントを検出しました。(指摘部位：<X>,発生事象：<Y>)
[意味] 指定管理 NIC で障害イベントを検出したことを示します。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] 指摘部位が"-"の場合は，対処の必要はありません。 指摘部位が"-"以外の場合は，以下の確認を行ってください。 (1) 管理 NIC の指定が正しいことを確認してください。 (2) (1)で問題ない場合は，指摘部位に共有モードをサポートしている NIC が搭載されていることを確認してください。		
FF42	警告	指定管理 NIC で警告イベントを検出しました。(指摘部位：<X>,発生事象：<Y>)
[意味] 指定管理 NIC で警告イベントを検出したことを示します。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] 指摘部位が"-"の場合は，対処の必要はありません。 指摘部位が"-"以外の場合は，以下の確認を行ってください。 (1) 管理 NIC の指定が正しいことを確認してください。 (2) (1)で問題ない場合は，指摘部位に共有モードをサポートしている NIC が搭載されていることを確認してください。		
FF43	情報	ユーザ指定の HVM 管理 NIC で HVM を起動しました。(指摘部位：<X>)
[意味] ユーザ指定の HVM 管理 NIC で HVM を起動したことを示します。 <X>は指摘部位を示します。 [対処] 特にありません。		
FF44	障害	管理 NIC で障害イベントが発生しました。(指摘部位：<X>,発生事象：<Y>)
[意味] 管理 NIC の Active ポートで障害を検出しました。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] 以下の確認を行ってください。 (1) 指摘部位の管理 NIC のポートからマネジメントモジュールまでのケーブル・スイッチが正しく設定・動作していることを確認してください。確認後，即時診断を実施してください。		

ID	レベル	メッセージ
内容		
(2) 管理 NIC が非冗長設定，もしくは管理 NIC の両ポートで本イベントが発生している場合は，マネジメントモジュールに関する障害が発生していないか確認してください。この場合は，マネジメントモジュールの障害対応を行ってください。		
FF45	警告	管理 NIC で警告イベントが発生しました。(指摘部位 : <X>,発生事象 : <Y>)
[意味] 管理 NIC の Standby ポートで障害を検出しました。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] 以下の確認を行ってください。 (1) 指摘部位の管理 NIC のポートからマネジメントモジュールまでのケーブル・スイッチが正しく設定・動作していることを確認してください。確認後，即時診断を実施してください。 (2) 管理 NIC が非冗長設定，もしくは管理 NIC の両ポートで本イベントが発生している場合は，マネジメントモジュールに関する障害が発生していないか確認してください。この場合は，マネジメントモジュールの障害対応を行ってください。		
FF46	情報	管理 NIC でイベントが発生しました。(指摘部位 : <X>,発生事象 : <Y>)
[意味] 管理 NIC でイベントが発生したことを示します。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] 発生事象が Switched between active and standby の場合は，管理 NIC/ポートの冗長性がなくなった可能性があります。管理 NIC に関する障害レベルのアラートがあればその対処を行ってください。 発生事象が Switched between active and standby 以外の場合は，対処の必要はありません。		
FF47	警告	ポート番号重複のため一部機能が利用できません。(指摘部位 : <X>,機能 : <Y>)
[意味] ポート番号が重複したため HVM の一部の機能が利用不能になっていることを示します。 <X>は指摘部位，<Y>は発生事象を示します。 [対処]ポート番号の設定を見直してください。		
FF48	情報	ポート番号重複が解消しました。(指摘部位 : <X>,機能 : <Y>)
[意味]ポート番号の重複が解消し，HVM の機能が利用可能になったことを示します。 <X>は指摘部位，<Y>は発生事象を示します。 [対処] 特に必要ありません。		
FFC0	情報	管理モジュールが接続要求アラートを送信しました。
[意味] マネジメントモジュールから HCSM に対して接続要求を行ったことを示します。 [対処] 特に必要ありません。		
FFC1	情報	管理モジュールが接続確立アラートを送信しました。
[意味] マネジメントモジュールと HCSM の接続が確立したことを示します。 [対処] 特に必要ありません。		
FFC2	情報	管理モジュールが生死確認アラートを送信しました。
[意味] マネジメントモジュールと HCSM の，接続の確認用アラートです。 [対処] 特に必要ありません。		
FFC3	情報	<X>で Pre-configure<Y>を開始しました。
[意味] X に示すサーバブレードにおいて，Pre-configure を開始したことを示します。 Y は Pre-configure の種類を示します。 • acquisition：サーバブレードより情報を取得するための Pre-configure • setting：サーバブレードに情報を設定するための Pre-configure • diagnosis：サーバブレードをテストするための Pre-configure [対処] 特に必要ありません。		
FFC4	情報	<X>で Pre-configure<Y>が成功しました。

ID	レベル	メッセージ
内容		
[意味] X に示すサーバブレードにおいて，Pre-configure が成功したことを示します。 Y は Pre-configure の種類を示します（メッセージ ID：FFC3 参照）。 [対処] 特に必要ありません。		
FFC5	情報	<X>で Pre-configure<Y>が失敗しました。
[意味] X に示すサーバブレードにおいて，Pre-configure が失敗したことを示します。 Y は Pre-configure の種類を示します（メッセージ ID：FFC3 参照）。 [対処] 失敗理由を示す別のアラートが通知されます。そのアラートの対処に従ってください。		
FFCA	情報	管理モジュールの IP アドレスが変更されました。
[意味] マネジメントモジュールの IP アドレスが変更されたことを示します。 [対処] 特に必要ありません。		
FFCB	情報	<X>のモジュール情報に変更がありました。
[意味] 装置のモジュール情報が更新されたことを示します。 [対処] 特に必要ありません。		
FFCC	情報	<X>のモジュール情報(構成設定)に変更がありました。
[意味] 装置のモジュール情報が更新されたことを示します。 [対処] 特に必要ありません。		
FFCD	情報	装置情報に変更がありました。
[意味] 装置情報が更新されたことを示します。 [対処] 特に必要ありません。		